

API Gateway

API Reference

Issue	03
Date	2025-08-27



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

Contents

1 Before You Start.....

2 API Overview.....

3 Calling APIs.....

3.1 Making an API Request.....

3.2 Authentication.....

3.3 Response.....

4 Dedicated Gateway APIs (V2).....

4.1 API Group Management.....

4.1.1 Creating an API Group.....

4.1.2 Modifying an API Group.....

4.1.3 Deleting an API Group.....

4.1.4 Querying API Group Details.....

4.1.5 Querying API Groups.....

4.1.6 Verifying an API Group Name.....

4.2 Environment Management.....

4.2.1 Creating an Environment.....

4.2.2 Modifying an Environment.....

4.2.3 Deleting an Environment.....

4.2.4 Querying Environments.....

4.3 Environment Variable Management.....

4.3.1 Creating a Variable.....

4.3.2 Deleting a Variable.....

4.3.3 Querying Variable Details.....

4.3.4 Querying Environment Variables.....

4.3.5 Modifying a Variable.....

4.4 Request Throttling Policy Management.....

4.4.1 Creating a Request Throttling Policy.....

4.4.2 Modifying a Request Throttling Policy.....

4.4.3 Deleting a Request Throttling Policy.....

4.4.4 Querying Request Throttling Policies.....

4.4.5 Querying Details of a Request Throttling Policy.....

4.5 API Management.....

1

3

9

9

11

13

15

15

15

23

31

34

41

49

53

53

57

61

64

68

68

74

77

80

85

90

90

97

104

107

113

118

4.5.1 Creating an API.....	118
4.5.2 Modifying an API.....	170
4.5.3 Deleting an API.....	218
4.5.4 Publishing an API or Taking an API Offline.....	221
4.5.5 Querying API Details.....	225
4.5.6 Querying APIs.....	252
4.5.7 Verifying the API Definition.....	271
4.5.8 Debugging an API.....	275
4.5.9 Publishing APIs or Taking APIs Offline.....	282
4.5.10 Querying Historical Versions of an API.....	287
4.5.11 Switching the Version of an API.....	292
4.5.12 Querying the Runtime Definition of an API.....	296
4.5.13 Querying API Version Details.....	306
4.5.14 Taking an API Version Offline.....	333
4.6 Signature Key Management.....	336
4.6.1 Creating a Signature Key.....	336
4.6.2 Modifying a Signature Key.....	346
4.6.3 Deleting a Signature Key.....	356
4.6.4 Querying Signature Keys.....	359
4.7 Binding/Unbinding Signature Keys.....	367
4.7.1 Binding a Signature Key.....	367
4.7.2 Unbinding a Signature Key.....	375
4.7.3 Querying Signature Keys Bound to an API.....	378
4.7.4 Querying APIs Not Bound with a Signature Key.....	386
4.7.5 Querying APIs Bound with a Signature Key.....	391
4.8 Binding/Unbinding Request Throttling Policies.....	397
4.8.1 Binding a Request Throttling Policy.....	397
4.8.2 Unbinding a Request Throttling Policy.....	401
4.8.3 Querying APIs Bound with a Request Throttling Policy.....	404
4.8.4 Querying APIs Not Bound with a Request Throttling Policy.....	410
4.8.5 Querying Request Throttling Policies Bound to an API.....	416
4.8.6 Unbinding Request Throttling Policies.....	422
4.9 Excluded Request Throttling Configuration.....	426
4.9.1 Creating an Excluded Request Throttling Configuration.....	426
4.9.2 Modifying an Excluded Request Throttling Configuration.....	431
4.9.3 Deleting an Excluded Request Throttling Configuration.....	435
4.9.4 Querying Excluded Request Throttling Configurations.....	439
4.10 App Authorization Management.....	443
4.10.1 Authorizing Apps.....	444
4.10.2 Canceling Authorization.....	449
4.10.3 Querying APIs Bound with an App.....	452
4.10.4 Querying APIs Not Bound with an App.....	458

4.10.5 Querying Apps Bound to an API.....	464
4.11 Resource Query.....	470
4.11.1 Querying API Quantities.....	470
4.11.2 Querying API Group Quantities.....	473
4.11.3 Querying App Quantities.....	477
4.12 Domain Name Management.....	480
4.12.1 Binding a Domain Name.....	481
4.12.2 Adding a Certificate to a Domain Name.....	488
4.12.3 Modifying a Domain Name.....	493
4.12.4 Unbinding a Domain Name.....	501
4.12.5 Setting Accessibility of a Debugging Domain Name.....	504
4.12.6 Deleting the Certificate Bound to a Domain Name.....	507
4.12.7 Querying Details of the Certificate Bound to a Domain Name.....	511
4.13 Access Control Policy Management.....	515
4.13.1 Creating an Access Control Policy.....	515
4.13.2 Modifying an Access Control Policy.....	520
4.13.3 Deleting an Access Control Policy.....	525
4.13.4 Deleting Multiple Access Control Policies.....	529
4.13.5 Querying Details of an Access Control Policy.....	533
4.13.6 Querying Access Control Policies.....	537
4.14 Binding/Unbinding Access Control Policies.....	542
4.14.1 Binding an Access Control Policy to an API.....	542
4.14.2 Unbinding an Access Control Policy.....	546
4.14.3 Unbinding Access Control Policies.....	549
4.14.4 Querying APIs Bound with an Access Control Policy.....	554
4.14.5 Querying APIs Not Bound with an Access Control Policy.....	559
4.14.6 Querying Access Control Policies Bound to an API.....	565
4.15 Custom Authorizer Management.....	570
4.15.1 Creating a Custom Authorizer.....	570
4.15.2 Modifying a Custom Authorizer.....	576
4.15.3 Deleting a Custom Authorizer.....	583
4.15.4 Querying Custom Authorizer Details.....	586
4.15.5 Querying Custom Authorizers.....	591
4.16 API Import and Export.....	597
4.16.1 Exporting APIs.....	597
4.16.2 Importing APIs.....	602
4.17 VPC Channel Management.....	608
4.17.1 Creating a VPC Channel.....	608
4.17.2 Updating a VPC Channel.....	635
4.17.3 Deleting a VPC Channel.....	662
4.17.4 Querying VPC Channel Details.....	666
4.17.5 Querying VPC Channels.....	683

4.17.6 Adding or Updating Backend Instances.....	697
4.17.7 Querying Backend Servers of a VPC Channel.....	705
4.17.8 Updating Backend Instances.....	711
4.17.9 Removing a Backend Server.....	720
4.17.10 Enabling Backend Servers.....	723
4.17.11 Disabling Backend Servers.....	727
4.17.12 Modifying VPC Channel Health Check.....	730
4.17.13 Adding or Updating a Backend Server Group of a VPC Channel.....	738
4.17.14 Querying Backend Server Groups of a VPC Channel.....	747
4.17.15 Querying a Backend Server Group of a VPC Channel.....	754
4.17.16 Deleting a Backend Server Group of a VPC Channel.....	759
4.17.17 Updating a Backend Server Group of a VPC Channel.....	762
4.18 Monitoring Information Query.....	770
4.18.1 Querying API Calls Within a Period.....	770
4.18.2 Querying Monitoring Data.....	776
4.18.3 Querying API Calls Under an API Group in the Last One Hour.....	782
4.19 Group Response Management.....	787
4.19.1 Creating a Group Response.....	787
4.19.2 Querying Group Response Details.....	797
4.19.3 Modifying a Group Response.....	804
4.19.4 Deleting a Group Response.....	814
4.19.5 Querying the Response of an Error Type.....	818
4.19.6 Modifying the Response of an Error Type.....	824
4.19.7 Deleting the Response of an Error Type.....	831
4.19.8 Querying Group Responses.....	836
4.20 Tag Management.....	843
4.20.1 Querying API Tags.....	843
4.21 Gateway Feature Management.....	847
4.21.1 Configuring a Feature for a Gateway.....	847
4.21.2 Querying Gateway Features.....	851
4.21.3 Querying the Supported Features of a Gateway.....	856
4.22 Configuration Management.....	859
4.22.1 Querying Resource Configurations of a Gateway.....	860
4.22.2 Querying Gateway Configurations.....	867
4.23 Gateway Management.....	871
4.23.1 Creating a Dedicated Gateway (Pay-Per-Use).....	871
4.23.2 Querying Dedicated Gateway Details.....	882
4.23.3 Updating a Dedicated Gateway.....	895
4.23.4 Querying the Creation Progress of a Dedicated Gateway.....	909
4.23.5 Updating or Binding an EIP to a Dedicated Gateway.....	913
4.23.6 Unbinding the EIP of a Dedicated Gateway.....	917
4.23.7 Enabling Public Access for a Dedicated Gateway.....	920

4.23.8 Updating the Outbound Access Bandwidth of a Dedicated Gateway.....	924
4.23.9 Disabling Public Access for a Dedicated Gateway.....	927
4.23.10 Enabling Public Inbound Access.....	930
4.23.11 Updating Public Inbound Access Bandwidth of a Gateway.....	934
4.23.12 Disabling Public Inbound Access for a Gateway.....	938
4.23.13 Querying AZs.....	941
4.23.14 Querying Dedicated Gateways.....	945
4.23.15 Deleting a Dedicated Gateway.....	955
4.23.16 Modifying the Specifications of a Pay-Per-Use Gateway.....	958
4.23.17 Querying Gateway Constraints.....	961
4.24 VPC Endpoint Management.....	964
4.24.1 Querying VPC Endpoint Connections.....	964
4.24.2 Accepting or Rejecting a VPC Endpoint Connection.....	970
4.24.3 Querying Whitelist Records of a VPC Endpoint Service.....	975
4.24.4 Adding Whitelist Records for a VPC Endpoint Service.....	979
4.24.5 Deleting Whitelist Records of a VPC Endpoint Service.....	984
4.25 Gateway Tag Management.....	988
4.25.1 Querying All Gateway Tags of a Project.....	988
4.25.2 Querying Tags of a Gateway.....	991
4.25.3 Adding or Deleting Tags of a Gateway.....	995
4.25.4 Querying the Number of Gateways with a Specified Tag.....	998
4.25.5 Querying Gateways by Tag.....	1003
4.26 Microservice Center Management.....	1009
4.26.1 Importing a Microservice.....	1009
4.27 SSL Certificate Management.....	1022
4.27.1 Querying SSL Certificates.....	1022
4.27.2 Creating an SSL Certificate.....	1027
4.27.3 Binding a Domain Name with SSL Certificates.....	1033
4.27.4 Unbinding a Domain Name's SSL Certificates.....	1036
4.27.5 Querying Certificate Details.....	1040
4.27.6 Deleting an SSL Certificate.....	1045
4.27.7 Modifying an SSL Certificate.....	1048
4.27.8 Binding an SSL Certificate to a Domain Name.....	1054
4.27.9 Unbinding an SSL Certificate from a Domain Name.....	1057
4.27.10 Querying Domain Names of an SSL Certificate.....	1061
4.28 Plug-in Management.....	1067
4.28.1 Creating a Plug-in.....	1067
4.28.2 Modifying a Plug-in.....	1077
4.28.3 Deleting a Plug-in.....	1086
4.28.4 Querying Plug-ins.....	1090
4.28.5 Querying Plug-in Details.....	1095
4.28.6 Binding a Plug-in to APIs.....	1100

4.28.7 Binding an API with Plug-ins.....	1105
4.28.8 Unbinding a Plug-in from All APIs.....	1110
4.28.9 Unbinding an API's Plug-ins.....	1113
4.28.10 Querying APIs Bound with a Plug-in.....	1117
4.28.11 Querying Plug-ins Bound to an API.....	1124
4.28.12 Querying APIs to Which a Plug-in Can Be Bound.....	1130
4.28.13 Querying Plug-ins That Can Be Bound to an API.....	1137
4.29 Credential Management.....	1142
4.29.1 Creating an App.....	1142
4.29.2 Modifying an App.....	1147
4.29.3 Deleting an App.....	1152
4.29.4 Resetting the AppSecret of an App.....	1155
4.29.5 Verifying an App.....	1160
4.29.6 Querying App Details.....	1163
4.29.7 Querying Apps.....	1168
4.29.8 Creating an AppCode.....	1173
4.29.9 Generating an AppCode.....	1177
4.29.10 Deleting an AppCode.....	1181
4.29.11 Querying AppCode Details.....	1184
4.29.12 Querying AppCodes of an App.....	1188
4.29.13 Querying Quotas Associated with a Credential.....	1193
4.29.14 Configuring Access Control Settings for an App.....	1197
4.29.15 Querying Access Control Details About an App.....	1201
4.29.16 Deleting Access Control Settings of an App.....	1205
4.30 Credential Quota Management.....	1208
4.30.1 Creating a Credential Quota.....	1208
4.30.2 Querying Credential Quota Details.....	1213
4.30.3 Querying Credential Quotas.....	1217
4.30.4 Modifying a Credential Quota.....	1221
4.30.5 Deleting a Credential Quota.....	1226
4.30.6 Querying the Credentials Bound to a Specified Quota.....	1230
4.30.7 Binding a Credential Quota with Credentials.....	1235
4.30.8 Unbinding a Credential Quota from a Credential.....	1239
4.30.9 Querying Credentials That Can Be Bound to a Credential Quota.....	1242
4.31 Asynchronous Task Management.....	1247
4.31.1 Exporting APIs Asynchronously.....	1247
4.31.2 Importing APIs Asynchronously.....	1252
4.31.3 Querying the Result of an Asynchronous Task.....	1256
4.32 Orchestration Rule Management.....	1261
4.32.1 Creating an Orchestration Rule.....	1261
4.32.2 Viewing Orchestration Rules.....	1274
4.32.3 Querying Rule Details.....	1280

4.32.4 Updating an Orchestration Rule.....	1287
4.32.5 Deleting an Orchestration Rule.....	1297
4.32.6 Querying APIs to Which an Orchestration Rule Is Bound.....	1301
4.33 Gateway Custom Inbound Port Management.....	1306
4.33.1 Querying the Domain Name Bound to a Custom Inbound Port.....	1306
4.33.2 Querying the Custom Inbound Ports of a Gateway.....	1311
4.33.3 Adding an Inbound Port for a Gateway.....	1315
4.33.4 Deleting an Inbound Port of a Gateway.....	1319
5 Shared Gateway APIs (for Existing Users).....	1323
5.1 API Group Management.....	1323
5.1.1 Object Model.....	1323
5.1.2 Creating an API Group.....	1325
5.1.3 Modifying an API Group.....	1328
5.1.4 Deleting an API Group.....	1331
5.1.5 Querying Details of an API Group.....	1332
5.1.6 Querying the API Group List.....	1334
5.2 API Management.....	1338
5.2.1 Object Model.....	1338
5.2.2 Creating an API.....	1349
5.2.3 Modifying an API.....	1370
5.2.4 Deleting an API.....	1391
5.2.5 Publishing an API.....	1392
5.2.6 Taking an API Offline.....	1394
5.2.7 Publishing Multiple APIs or Taking Multiple APIs Offline.....	1395
5.2.8 Querying API Details.....	1398
5.2.9 Querying an API List.....	1407
5.2.10 Querying Historical API Versions.....	1411
5.2.11 Taking an Effective Version of an API Offline.....	1413
5.2.12 Querying Details of an API Version.....	1414
5.2.13 Querying the Runtime Definition of an API.....	1421
5.2.14 Debugging an API.....	1425
5.3 App Management.....	1430
5.3.1 Object Model.....	1430
5.3.2 Creating an App.....	1431
5.3.3 Modifying an App.....	1433
5.3.4 Resetting an AppSecret.....	1436
5.3.5 Deleting an App.....	1438
5.3.6 Verifying an App.....	1439
5.3.7 Querying App Details.....	1440
5.3.8 Querying an App List.....	1442
5.3.9 Creating an AppCode.....	1445
5.3.10 Generating an AppCode.....	1447

5.3.11 Querying AppCode Details.....	1448
5.3.12 Querying an AppCode List.....	1450
5.3.13 Deleting an AppCode.....	1452
5.4 App Authorization Management.....	1453
5.4.1 Object Model.....	1453
5.4.2 Querying the List of APIs Not Bound to an App.....	1454
5.4.3 Authorizing Apps.....	1456
5.4.4 Querying the List of APIs Bound to an App.....	1458
5.4.5 Querying the List of Apps Bound to an API.....	1461
5.4.6 Canceling Authorization.....	1464
5.5 Environment Management.....	1465
5.5.1 Object Model.....	1465
5.5.2 Creating an Environment.....	1466
5.5.3 Modifying an Environment.....	1467
5.5.4 Deleting an Environment.....	1469
5.5.5 Querying an Environment List.....	1470
5.6 Environment Variable Management.....	1472
5.6.1 Object Model.....	1472
5.6.2 Creating an Environment Variable.....	1473
5.6.3 Deleting an Environment Variable.....	1475
5.6.4 Querying Environment Variable Details.....	1476
5.6.5 Querying an Environment Variable List.....	1478
5.7 Request Throttling Policy Management.....	1480
5.7.1 Object Model.....	1480
5.7.2 Creating a Request Throttling Policy.....	1482
5.7.3 Modifying a Request Throttling Policy.....	1486
5.7.4 Deleting a Request Throttling Policy.....	1490
5.7.5 Querying Details of a Request Throttling Policy.....	1491
5.7.6 Querying the Request Throttling Policy List.....	1494
5.8 Binding Request Throttling Policies.....	1497
5.8.1 Object Model.....	1497
5.8.2 Querying the List of APIs Not Bound to a Request Throttling Policy.....	1498
5.8.3 Binding a Request Throttling Policy.....	1501
5.8.4 Querying the List of APIs Bound to a Request Throttling Policy.....	1503
5.8.5 Querying the List of Request Throttling Policies Bound to an API.....	1506
5.8.6 Unbinding a Request Throttling Policy.....	1509
5.9 Excluded Request Throttling Configuration.....	1510
5.9.1 Object Model.....	1510
5.9.2 Creating an Excluded Request Throttling Configuration.....	1511
5.9.3 Modifying an Excluded Request Throttling Configuration.....	1513
5.9.4 Deleting an Excluded Request Throttling Configuration.....	1515
5.9.5 Querying the List of Excluded Request Throttling Configurations.....	1516

5.10 Access Control Policy Management.....	1519
5.10.1 Object Model.....	1519
5.10.2 Creating an Access Control Policy.....	1520
5.10.3 Modifying an Access Control Policy.....	1522
5.10.4 Deleting an Access Control Policy.....	1524
5.10.5 Deleting Multiple Access Control Policies.....	1525
5.10.6 Querying Details of an Access Control Policy.....	1527
5.10.7 Querying the Access Control Policy List.....	1529
5.11 Binding Access Control Policies.....	1531
5.11.1 Object Model.....	1531
5.11.2 Binding an Access Control Policy to an API.....	1532
5.11.3 Querying the List of Access Control Policies Bound to an API.....	1534
5.11.4 Querying the List of APIs Bound to an Access Control Policy.....	1536
5.11.5 Querying the List of APIs Not Bound to an Access Control Policy.....	1539
5.11.6 Unbinding an Access Control Policy from an API.....	1542
5.11.7 Unbinding Multiple Access Control Policies from APIs.....	1543
5.12 Querying Subscription Information in KooGallery.....	1545
5.12.1 Querying the List of Purchased API Groups.....	1545
5.12.2 Querying Details of a Purchased API Group.....	1548
5.12.3 Querying the List of Purchased APIs.....	1549
5.13 Configuration Management.....	1552
5.13.1 Object Model.....	1552
5.13.2 Querying Configuration Details.....	1553
5.14 Resource Query.....	1555
5.14.1 Querying API Group Quantities.....	1555
5.14.2 Querying API Quantities.....	1556
5.14.3 Querying App Quantities.....	1558
5.15 Signature Key Management.....	1559
5.15.1 Object Model.....	1559
5.15.2 Creating a Signature Key.....	1559
5.15.3 Modifying a Signature Key.....	1561
5.15.4 Deleting a Signature Key.....	1563
5.15.5 Querying the Signature Key List.....	1564
5.16 Binding Signature Keys.....	1567
5.16.1 Object Model.....	1567
5.16.2 Querying the List of APIs Not Bound to a Signature Key.....	1567
5.16.3 Binding a Signature Key.....	1570
5.16.4 Querying the List of APIs Bound to a Signature Key.....	1572
5.16.5 Querying the List of Signature Keys Bound to an API.....	1575
5.16.6 Unbinding a Signature Key.....	1578
5.17 Domain Name Management.....	1579
5.17.1 Object Model.....	1579

5.17.2 Binding a Domain Name.....	1580
5.17.3 Unbinding a Domain Name.....	1582
5.17.4 Adding a Certificate to a Domain Name.....	1583
5.17.5 Deleting a Certificate Bound to a Domain Name.....	1585
5.17.6 Querying Details of a Certificate Bound to a Domain Name.....	1586
5.18 VPC Channel Management.....	1588
5.18.1 Object Model.....	1588
5.18.2 Creating a VPC Channel.....	1591
5.18.3 Updating a VPC Channel.....	1596
5.18.4 Deleting a VPC Channel.....	1601
5.18.5 Querying VPC Channel Details.....	1602
5.18.6 Querying the VPC channel List.....	1606
5.18.7 Adding Backend Instances (Cloud Servers).....	1609
5.18.8 Deleting a Backend Instance (Cloud Server).....	1612
5.18.9 Querying the Backend Instance List (Cloud Server List).....	1613
5.19 Querying Metrics.....	1616
5.19.1 Querying API Calls Within a Period.....	1616
5.19.2 Querying API Calls Under an API Group in the Last One Hour.....	1619
5.20 OpenAPI.....	1622
5.20.1 Exporting All APIs in an API Group.....	1622
5.20.2 Exporting Multiple APIs.....	1635
5.20.3 Importing APIs to a New API Group.....	1648
5.20.4 Importing APIs to an Existing API Group.....	1662
5.21 Custom Authorizer Management.....	1677
5.21.1 Creating a Custom Authorizer.....	1677
5.21.2 Modifying a Custom Authorizer.....	1680
5.21.3 Deleting a Custom Authorizer.....	1683
5.21.4 Querying Details of a Custom Authorizer.....	1684
5.21.5 Querying a Custom Authorizer List.....	1686
6 Permissions Policies and Supported Actions.....	1690
7 Appendix.....	1712
7.1 Pagination Query.....	1712
7.2 Result Filtering.....	1712
7.3 HTTP Status Codes.....	1712
7.4 Error Codes.....	1714
7.5 Supported Features.....	1746
7.6 Obtaining a Project ID.....	1766
7.7 Obtaining an Account Name and Account ID.....	1768
7.8 Data Structure (Plugin Content Definition).....	1768
7.8.1 CorsPluginContent.....	1768
7.8.2 SetRespHeadersContent.....	1769
7.8.3 KafkaLogContent.....	1770

API Gateway

API Reference

Contents

7.8.4 BreakerContent.....

7.8.5 RateLimitContent.....

7.8.6 ThirdAuthContent.....

7.8.7 ProxyCacheContent.....

7.8.8 ProxyMirrorContent.....

8 Change History.....

1778

1788

1791

1796

1799

1801

1 Before You Start

API Gateway (APIG) is a high-performance, high-availability, and high-security API hosting service that helps enterprises build, manage, and deploy APIs at any scale.

This document describes how to use REST APIs to perform operations on APIG, such as creating, deleting, and modify your own APIs. For details about all supported operations, see [API Overview](#).

If you plan to access API Gateway through APIs, ensure that you are familiar with API Gateway concepts. For details, see the [Service Overview](#).

NOTE

V2.0 APIs are provided for the dedicated gateways and V1.0 APIs are provided for the shared gateway on the old console. The shared gateway on the old console has been removed. Please use dedicated gateways to manage your APIs instead.

Endpoints

An endpoint is the request address for calling an API. Endpoints vary depending on services and regions. For the endpoints of all services, see [Regions and Endpoints](#).

Concepts

- **Account**
An account is created upon successful registration with Huawei Cloud. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity and should not be used directly to perform routine management. For security purposes, create IAM users and grant them permissions for routine management.
- **IAM user**
A user is created using a domain to use cloud services. Each user has its own identity credentials (password and access keys).
An IAM user can view the account ID and user ID on the [My Credentials](#) page of the console. The domain name, username, and password will be required for API authentication.
- **Region**

Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.

For details, see [Regions and AZs](#).

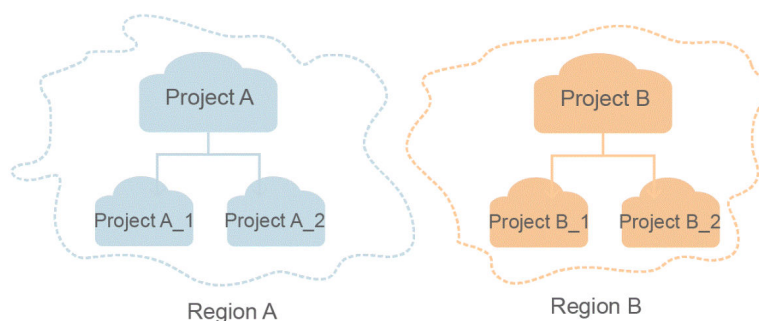
- Availability zone (AZ)

An Availability Zone (AZ) contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, compute, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to support cross-AZ high-availability systems.

- Project

Projects group and isolate resources (including compute, storage, and network resources) across physical regions. A default project is provided for each Huawei Cloud region, and subprojects can be created under each default project. Users can be granted permissions to access all resources in a specific project. If you need more refined access control, create subprojects under a default project and create resources in subprojects. Then you can assign users the permissions required to access only the resources in the specific subprojects.

Figure 1-1 Project isolating model



An IAM user can view the project ID on the [My Credentials](#) page of the console.

- Enterprise project

Enterprise projects group and manage resources across regions. Resources in different enterprise projects are logically isolated. An enterprise project can contain resources of multiple regions, and resources can be added to or removed from enterprise projects.

For details about how to obtain enterprise project IDs and features, see the [Enterprise Management Service User Guide](#).

2 API Overview

[Table 2-1](#) describes the types and descriptions of dedicated gateway APIs. [Table 2-2](#) describes the types and descriptions of the shared gateway APIs.

Table 2-1 Overview of dedicated gateway APIs

Type	Description
API Group Management	Create, modify, delete, and query API groups.
Environment Management	Create, modify, delete, and query environments.
Environment Variable Management	Create, modify, delete, query, and list environment variables.
Request Throttling Policy Management	Create, modify, delete, and query request throttling policies.
API Management	Create, modify, delete, publish, query, and debug APIs, take APIs offline, verify API definitions, and switch API versions.
Signature Key Management	Create, modify, delete, and query signature keys.
Binding/Unbinding Signature Keys	Bind and unbind signature keys, query signature keys bound to an API, and query APIs that are bound or not bound with a signature key.
Binding/Unbinding Request Throttling Policies	Bind and unbind request throttling policies, query APIs that are bound or not bound with a request throttling policy, and query request throttling policies bound to an API.

Type	Description
Excluded Request Throttling Configuration	Create, modify, delete, and query excluded request throttling configurations.
App Authorization Management	Authorize apps, cancel authorizations, query APIs that are bound or not bound with an app, and query apps bound to an API.
Resource Query	Query the quantities of APIs, API groups, and apps.
Domain Name Management	Bind, modify, and unbind domain names; bind, delete, and query domain name certificates.
Access Control Policy Management	Create, modify, delete, and query access control policies.
Binding/Unbinding Access Control Policies	Bind and unbind access control policies, query APIs that are bound or not bound with an access control policy, and query access control policies bound to an API.
Custom Authorizer Management	Create, modify, delete, and query custom authorizers.
API Import and Export	Import and export APIs.
VPC Channel Management	Includes: • Create, update, delete, and query VPC channels. • Add, query, and delete backend servers. • Enabling/Disabling backend servers. • Modify health check configuration of a VPC channel. • Add, update, delete, and view backend server groups, and query backend server group list of a VPC channel.
Monitoring Information Query	Query API calls within a specific period and query API calls under an API group in the last one hour.
Group Response Management	Create, query, modify, and delete group responses; query, modify, and delete responses of an error type.

Type	Description
Tag Management	Query tags.
Gateway Feature Management	Configure and query gateway features.
Configuration Management	Query resource configurations of a gateway and query gateway configurations.
Gateway Management	Includes: • Create, update, query, and delete dedicated gateways. • Bind and unbind EIPs. • Enable or disable public access for dedicated gateways, and update the outbound access bandwidth of dedicated gateways. • Query AZs. • Modify specifications. • Query gateway constraints.
VPC Endpoint Management	Includes: • Query the VPC endpoint connections of a gateway. • Query the whitelist records of a gateway's VPC endpoint service. • Accept or reject a VPC endpoint connection for a gateway. • Add whitelist records in batches for or delete those of a gateway's VPC endpoint service.
Gateway Tag Management	Add, delete, and query gateway tags.
Microservice Center Management	Import microservices.
SSL Certificate Management	Includes: • Create, delete, modify, and view a certificate, and query all SSL certificates. • Bind or unbind a domain name's SSL certificates. • Bind an SSL certificate to or unbind it from a domain name. • Obtain domain names bound to an SSL certificate.

Type	Description
Plug-in Management	Includes: • Create, modify, delete, and view a plug-in, and query all plug-ins. • Bind a plug-in to or unbind it from APIs. • Bind or unbind an API's plug-ins. • Query APIs bound with a plug-in or query plug-ins bound to an API. • Query APIs to which a plug-in can be bound or query plug-ins that can be bound to an API.
Credential Management	Includes: • Create, modify, delete, verify, and query apps, and reset AppKeys. • Create, automatically generate, delete, and query AppCodes. • Query the quotas of a credential. • Configure and delete access control settings of an app, and query access control details of an app.
Credential Quota Management	Includes: • Create, modify, and delete a credential quota. • Query credential quota details and all credential quotas. • Bind a credential quota to a credential, or unbind a quota from a specified credential. • Query credentials bound or not bound with a specified quota.
Asynchronous Task Management	Includes: • Import or export APIs asynchronously. • Query the result of an asynchronous task.
Orchestration Rule Management	Includes: • Create, view, update, and delete orchestration rules, and query orchestration rule details. • Query APIs to which an orchestration rule is bound.
Gateway Custom Inbound Port Management	Includes: • Add or delete a custom inbound port. • Query custom inbound ports of a gateway. • Query the domain names bound to a custom inbound port.

Table 2-2 Overview of shared gateway APIs (for existing users)

Type	Description
API Group Management	Create, modify, delete, and query API groups.
API Management	Create, modify, delete, publish, and query APIs, and take APIs offline.
App Management	Create, modify, delete, and query apps, and reset AppSecrets.
App Authorization Management	Authorize apps and cancel and query authorizations.
Environment Management	Create, modify, delete, and query environments.
Environment Variable Management	Create, delete, and query environment variables.
Request Throttling Policy Management	Create, modify, delete, and query request throttling policies.
Binding/Unbinding Request Throttling Policies	Query, bind, and unbind request throttling policies.
Excluded Request Throttling Configuration	Create, modify, delete, and query excluded request throttling configurations.
Access Control Policy Management	Create, modify, delete, and query blacklists and whitelists.
Binding Access Control Policies	Query access control policies bound to an API and APIs that are bound or not bound to an access control policy; unbind an API from an access control policy.
Querying Subscription Information in KooGallery	Query purchased API groups, API group details, and APIs.
Configuration Management	Configure object models and query configuration details.
Resource Query	Query the numbers of API groups, APIs, and apps.

Type	Description
Signature Key Management	Create, modify, delete, and query signature keys.
Binding/Unbinding Signature Keys	Bind and unbind signature keys; query APIs that are bound or not bound to a signature key; query signature keys bound to an API.
Domain Name Management	Bind and unbind domain names; bind and delete certificates.
VPC Channel Management	Create, update, delete, and query VPC channels; add, delete, and query cloud servers.
Monitoring Information Query	Query the number of times an API or APIs in an API group are called.
API Import and Export	Export Swagger definitions of APIs published in a specific environment.
Custom Authorizer Management	Create, modify, delete, and query custom authorizers.

3 Calling APIs

3.1 Making an API Request

This section describes the structure of a REST API request, and uses the APIG API for [creating an API group \(dedicated gateways\)](#) as an example to demonstrate how to call an API.

Request URI

A request URI is in the following format:

{URI-scheme}://{Endpoint} / {resource-path} ? {query-string}

Although a request URI is included in the request header, most programming languages or frameworks require the request URI to be transmitted separately.

- **URI-scheme:** Protocol used to transmit requests. All APIs use **HTTPS**.
- **Endpoint:** Domain name or IP address of the server bearing the REST service. It can be obtained from [Endpoints](#). For example, the endpoint of APIG in the **CN-Hong Kong** region is **apig.ap-southeast-1.myhuaweicloud.com**.
- **resource-path:** Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to create an API group (dedicated gateway) is **/v2/{project_id}/apigw/instances/{instance_id}/api-groups**. *{project_id}* indicates a [project ID](#) and *{instance_id}* indicates a gateway ID. The two IDs can be obtained from the gateway information on the APIG console.
- **query-string:** Query parameter, which is optional. Ensure that a question mark (?) is included in front of each query parameter that is in the format of *Parameter name=Parameter value*. For example, **limit=10** indicates that a maximum of 10 data records will be queried.

For example, if you want to create an API group in the **CN-Hong Kong** region, set **URI-scheme** to **HTTPS**, **Endpoint** to **apig.ap-southeast-1.myhuaweicloud.com**, and **resource-path** to **/v2/{project_id}/apigw/instances/{instance_id}/api-groups**. Combine the parameters in the URI.

`https://apig.ap-southeast-1.myhuaweicloud.com/v2/{project_id}/apigw/instances/{instance_id}/api-groups`

 NOTE

To simplify the URI display in this document, each API is provided only with a **resource-path** and a request method. The **URI-scheme** of all APIs is **HTTPS**, and the endpoints of all APIs in the same region are identical.

Request Method

The HTTP protocol defines the following request methods that can be used to send a request to the server:

- **GET**: requests the server to return specified resources.
- **PUT**: requests the server to update specified resources.
- **POST**: requests the server to add resources or perform special operations.
- **DELETE**: requests the server to delete specified resources, for example, an object.
- **HEAD**: same as GET except that the server must return only the response header.
- **PATCH**: requests the server to update partial content of a specified resource. If the resource does not exist, a new resource will be created.

For example, in the case of the API used to [create an API group](#), the request method is POST. The request is as follows:

```
POST https://apig.ap-southeast-1.myhuaweicloud.com/v2/{project_id}/apigw/instances/{instance_id}/api-groups
```

Request Header

You can also add additional header fields to a request, such as the fields required by a specified URI or HTTP method. For example, to request for the authentication information, add **Content-Type**, which specifies the request body type.

Common request header fields are as follows:

- **Content-Type**: specifies the request body type or format. This field is mandatory and its default value is **application/json**. Other values of this field will be provided for specific APIs if any.
- **X-Sdk-Date**: specifies the time when a request is sent. This field is optional. When AK/SK authentication is enabled, this field is automatically specified when SDK is used to sign the request. For more information, see [AK/SK-based Authentication](#).
- **Authorization**: specifies signature authentication information. This field is optional. When AK/SK authentication is enabled, this field is automatically specified when SDK is used to sign the request. For more information, see [AK/SK-based Authentication](#).
- **X-Auth-Token**: specifies a user token only for token-based API authentication. The user token is a response to the API used to [obtain a user token](#). This API is the only one that does not require authentication.
- **X-Project-ID**: specifies subproject ID. This field is optional and can be used in multi-project scenarios. The **X-Project-ID** field is mandatory in the request header for accessing resources in a sub-project through AK/SK-based authentication.

- **X-Domain-ID**: specifies account ID, which is optional. When you call APIs of global services using AK/SK-based authentication, **X-Domain-ID** needs to be configured in the request header.

If AK/SK authentication is used, the requests of the API used to [create an API group](#) with the added headers are as follows:

```
POST https://apig.ap-southeast-1.myhuaweicloud.com/v2/{project_id}/apigw/instances/{instance_id}/api-groups
Content-Type: application/json
X-Sdk-Date: 20240416T095341Z
Authorization: SDK-HMAC-SHA256 Access=*****, SignedHeaders=content-type;host;x-sdk-date,
Signature=*****
```

Request Body

The body of a request is often sent in a structured format as specified in **Content-Type**. The request body transfers content other than the request header. If the request body contains Chinese characters, set **Content-type** to **utf-8**, for example, Content-Type: application/json; charset=utf-8.

Request bodies vary between APIs. Some APIs do not require the request body, such as the APIs requested using the **GET** and **DELETE** methods.

For the API used to [create an API group](#), you can obtain the request parameters and parameter description from the API request. Here is an example request that includes a body. The bold fields must be configured as required.

- **name**: API group name
- **remark**: API group description

```
POST https://apig.ap-southeast-1.myhuaweicloud.com/v2/{project_id}/apigw/instances/{instance_id}/api-groups
POST https://{apig_endpoint}/v2/{project_id}/v2/{project_id}/apigw/instances/{instance_id}/api-groups
Content-Type: application/json
X-Sdk-Date: 20240416T095341Z
Authorization: SDK-HMAC-SHA256 Access=*****, SignedHeaders=content-type;host;x-sdk-date,
Signature=*****
{
  "name": "APIGroup_test",
  "remark": "api group remark"
}
```

If all data required for the API request is available, you can send the request to call the API through [curl](#), [Postman](#), or coding.

3.2 Authentication

Requests for calling an API can be authenticated using either of the following methods:

- **AK/SK-based authentication**: Requests are authenticated by encrypting the request body using an AK/SK pair. AK/SK-based authentication is recommended because it provides higher security than token-based authentication.
- **Token-based authentication**: Requests are authenticated using a token.

AK/SK-based Authentication

In AK/SK-based authentication, AK/SK is used to sign requests and the signature is then added to the requests for authentication.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

Constraints:

- AK/SK-based authentication supports API requests with a body not larger than 12 MB. For API requests with a larger body, token-based authentication is recommended.
- Tokens obtained using an AK/SK are valid for at least 15 minutes.
- Both AK/SK in a permanent access key or in a temporary access are supported. The **X-Security-Token** field must be configured when the AK/SK in the temporary access key is used, and the field value is the **security_token** of the temporary access key.

In AK/SK-based authentication, you can use an AK/SK to sign requests based on the signature algorithm or use the signing SDK to sign requests. For details about how to sign requests and use the signature SDK, see [API Request Signing Guide](#).

NOTICE

- The signing SDK is only used for signing requests and is different from the SDKs provided by services.
 - The local time on the client must be synchronized with the clock server to avoid a large offset in the value of the **X-Sdk-Date** request header.
 - APIG checks the time format and compares the time with the time when APIG receives the request. If the time difference exceeds 15 minutes, APIG will reject the request.
-

Token-based Authentication

NOTICE

- The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the IAM API used to obtain a user token.
 - Ensure that the token is valid when you use it. Using a token that will soon expire may cause API calling failures.
-

A token specifies temporary permissions in a computer system. During API authentication using a token, the token is added to requests to get permissions for calling the API.

When calling an API to [obtain a user token](#), you must set **auth.scope** in the request body to **project**.

```
{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "name": "username",
          "password": "*****",
          "domain": {
            "name": "domainname"
          }
        }
      }
    },
    "scope": {
      "project": {
        "name": "xxxxxxx"
      }
    }
  }
}
```

After a token is obtained, the **X-Auth-Token** header field must be added to requests to specify the token when calling other APIs. For example, if the token is **ABCDEFGH....**, **X-Auth-Token: ABCDEFGH....** can be added to a request as follows:

```
POST https://apig.ap-southeast-1.myhuaweicloud.com/v2/{project_id}/apigw/instances/{instance_id}/api-groups
POST https://{apig_endpoint}/v2/{project_id}/v2/{project_id}/apigw/instances/{instance_id}/api-groups
Content-Type: application/json
X-Auth-Token: ABCDEFGH....
```

3.3 Response

After sending a request, you will receive a response, including a status code, response header, and response body.

Status Code

A status code is a group of digits, ranging from 1xx to 5xx. It indicates the status of a request. For more information, see [HTTP Status Codes](#).

For example, if status code **201** is returned for calling the API used to [create an API group \(dedicated gateways\)](#), the request is successful.

Response Header

Similar to a request, a response also has a header, for example, **Content-Type**.

For example, when calling the API used to [create an API group \(dedicated gateways\)](#), the response headers are shown below.

Figure 3-1 Response headers for creating an API group

```
"X-Frame-Options": "SAMEORIGIN",  
"Strict-Transport-Security": "max-age=31536000; includeSubdomains;",  
"Server": "CloudWAF",  
"X-Request-Id": "6a838baac776594e4b0f1e258061ed95",  
"X-Content-Type-Options": "nosniff",  
"Connection": "keep-alive",  
"X-Download-Options": "noopen",  
"Set-Cookie": "WAFSESTIME=1716451295054; path=/",  
"X-XSS-Protection": "1; mode=block;",  
"Content-Length": "580",  
"Date": "Thu, 23 May 2024 08:01:38 GMT",  
"Content-Type": "application/json; charset=utf-8"
```

Response Body

The body of a response is often returned in structured format as specified in the **Content-Type** header field. The response body transfers content except the response header.

The following is part of the response body for the API used to **create an API group (dedicated gateways)**.

```
{  
  "id": "41e08fbaca9f4d64bde467d0dd89ff51",  
  "name": "aaa",  
  "status": 1,  
  "sl_domain": "41e08fbaca9f4d64bde467d0dd89ff51.example.cloudapis.com",  
  "register_time": "2024-05-23T08:03:56.419897855Z",  
  "update_time": "2024-05-23T08:03:56.419897962Z",  
  "on_sell_status": 2,  
  "url_domains": [],  
  "sl_domain_access_enabled": true,  
  "sl_domains": [  
    "41e08fbaca9f4d64bde467d0dd89ff51.example.cloudapis.com"  
  ],  
  "remark": "",  
  "call_limits": 0,  
  "time_interval": 0,  
  "time_unit": "",  
  "is_default": 2,  
  "version": ""  
}
```

If an error occurs during API calling, an error code and a message will be displayed. The following shows an error response body.

```
{  
  "error_msg": "The token is missing.",  
  "error_code": "APIG.1000"  
}
```

In the response body, **error_code** is an error code, and **error_msg** provides information about the error.

4 Dedicated Gateway APIs (V2)

4.1 API Group Management

4.1.1 Creating an API Group

Function

This API is used to create an API group. An API group is an API management unit and the entry to a service. A subdomain name is returned as the access entry when an API group is created. APIs in an API group should be correlated with each other.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/api-groups

Table 4-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-2 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-3 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	API group name. The value can contain 3 to 255 characters, including letters, digits, and special characters (-_./():). It must start with a letter or digit. Minimum: 3 Maximum: 255
remark	No	String	API group description. Maximum: 1000
roma_app_id	No	String	ID of the integration application to which the API group belongs. This parameter is required when the group version is V2. Currently, this parameter is not supported.
version	No	String	Group version. • V1: global group • V2: application-level group This parameter is not supported currently.

Response Parameters

Status code: 201

Table 4-4 Response body parameters

Parameter	Type	Description
id	String	ID.
name	String	API group name.
status	Integer	Status. • 1: valid
sl_domain	String	Subdomain name that APIG automatically allocates to the API group.
register_time	String	Creation time.
update_time	String	Last modification time.
on_sell_status	Integer	Indicates whether the API group has been listed on KooGallery. • 1: listed • 2: not listed • 3: under review Not supported currently.
url_domains	Array of UrlDomain objects	Independent domain names bound to the API group.
sl_domain_access_enabled	Boolean	Whether the debugging domain name is accessible. Options: true and false. Default: true
sl_domains	Array of strings	Automatically allocated subdomain names.
remark	String	Description.
call_limits	Integer	Total number of times all APIs in the API group can be accessed. Consider the payload capacity of the backend service when setting this parameter. By default, there is no limit on the number of API calls. Currently, this parameter is not supported.
time_interval	Integer	Period of time for limiting the number of API calls. Currently, this parameter is not supported.

Parameter	Type	Description
time_unit	String	Time unit for limiting the number of API calls. Currently, this parameter is not supported.
is_default	Integer	Indicates whether the API group is the default group.
version	String	Group version. • V1: global group • V2: application-level group This parameter is not supported currently.
roma_app_id	String	ID of the integration application to which the API group belongs. This parameter is required when the group version is V2. Currently, this parameter is not supported.
roma_app_name	String	Name of the integration application to which the API group belongs. Currently, this parameter is not supported.

Table 4-5 UrlDomain

Parameter	Type	Description
id	String	Domain ID.
domain	String	Domain name.
cname_status	Integer	CNAME resolution status of the domain name. • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
min_ssl_version	String	Minimum SSL version. TLS 1.1 and TLS 1.2 are supported. Default: TLSv1.1

Parameter	Type	Description
verified_client_certificate_enabled	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false
is_has_trusted_root_ca	Boolean	Whether a trusted root certificate (CA) exists. The value is true if trusted_root_ca exists in the bound certificate. Default: false
ingress_http_port	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151

Parameter	Type	Description
ingress_https_port	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ssl_infos	Array of SslInfo objects	SSL certificate list.

Table 4-6 SslInfo

Parameter	Type	Description
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2
type	String	Certificate scope: • instance • global Default: global

Status code: 400

Table 4-7 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-8** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-9** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-10** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Creating an API group

```
{
  "name" : "api_group_001",
  "remark" : "API group 1"
}
```

Example Responses

Status code: 201

Created

```
{
  "update_time" : "2020-07-31T06:55:55.383169299Z",
  "name" : "api_group_001",
  "on_sell_status" : 2,
  "remark" : "API group 1",
  "sl_domains" : [ "c77f5e81d9cb4424bf704ef2b0ac7600.apic.****.com",
    "c77f5e81d9cb4424bf704ef2b0ac7600.apic.****.cn" ],
  "sl_domain" : "c77f5e81d9cb4424bf704ef2b0ac7600.apic.****.com",
  "id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "register_time" : "2020-07-31T06:55:55.383169068Z",
  "status" : 1,
  "is_default" : 2,
  "sl_domain_access_enabled" : true
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request

Status Code	Description
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.1.2 Modifying an API Group

Function

This API is used to modify the attributes of an API group. Only the name and remark attributes of an API group can be modified.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}

Table 4-11 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.

Request Parameters

Table 4-12 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-13 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	API group name. The value can contain 3 to 255 characters, including letters, digits, and special characters (-_./():). It must start with a letter or digit. Minimum: 3 Maximum: 255
remark	No	String	API group description. Maximum: 1000

Response Parameters

Status code: 200

Table 4-14 Response body parameters

Parameter	Type	Description
id	String	ID.
name	String	API group name.
status	Integer	Status. 1: valid
sl_domain	String	Subdomain name that APIG automatically allocates to the API group.
register_time	String	Creation time.

Parameter	Type	Description
update_time	String	Last modification time.
on_sell_status	Integer	Indicates whether the API group has been listed on KooGallery. • 1: listed • 2: not listed • 3: under review Not supported currently.
url_domains	Array of UrlDomain objects	Independent domain names bound to the API group.
sl_domain_access_enabled	Boolean	Whether the debugging domain name is accessible. Options: true and false. Default: true
sl_domains	Array of strings	Automatically allocated subdomain names.
remark	String	Description.
call_limits	Integer	Total number of times all APIs in the API group can be accessed. Consider the payload capacity of the backend service when setting this parameter. By default, there is no limit on the number of API calls. Currently, this parameter is not supported.
time_interval	Integer	Period of time for limiting the number of API calls. Currently, this parameter is not supported.
time_unit	String	Time unit for limiting the number of API calls. Currently, this parameter is not supported.
is_default	Integer	Indicates whether the API group is the default group.
version	String	Group version. • V1: global group • V2: application-level group This parameter is not supported currently.

Parameter	Type	Description
roma_app_id	String	ID of the integration application to which the API group belongs. This parameter is required when the group version is V2. Currently, this parameter is not supported.
roma_app_name	String	Name of the integration application to which the API group belongs. Currently, this parameter is not supported.

Table 4-15 UrlDomain

Parameter	Type	Description
id	String	Domain ID.
domain	String	Domain name.
cname_status	Integer	CNAME resolution status of the domain name. • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
min_ssl_version	String	Minimum SSL version. TLS 1.1 and TLS 1.2 are supported. Default: TLSv1.1
verified_client_certificate_enabled	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false
is_has_trusted_root_ca	Boolean	Whether a trusted root certificate (CA) exists. The value is true if trusted_root_ca exists in the bound certificate. Default: false

Parameter	Type	Description
ingress_http_port	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ingress_https_port	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ssl_infos	Array of SslInfo objects	SSL certificate list.

Table 4-16 SslInfo

Parameter	Type	Description
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2
type	String	Certificate scope: • instance • global Default: global

Status code: 400**Table 4-17** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-18** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-19** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-20** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-21** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Modifying an API group

```
{
  "name" : "api_group_001",
  "remark" : "API group 1"
}
```

Example Responses**Status code: 200**

OK

```
{
  "update_time" : "2020-07-31T06:55:55Z.866474185Z",
  "name" : "api_group_001",
  "on_sell_status" : 2,
  "remark" : "API group 1",
  "sl_domains" : [ "c77f5e81d9cb4424bf704ef2b0ac7600.apic.***.com",
    "c77f5e81d9cb4424bf704ef2b0ac7600.apic.***.cn" ],
  "sl_domain" : "c77f5e81d9cb4424bf704ef2b0ac7600.apic.***.com",
  "id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "register_time" : "2020-07-31T06:55:55Z",
  "status" : 1,
  "is_default" : 2,
  "sl_domain_access_enabled" : true
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3001",
  "error_msg" : "API group c77f5e81d9cb4424bf704ef2b0ac7600 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.1.3 Deleting an API Group

Function

This API is used to delete an API group.

If the group to delete contains APIs, take the APIs offline and delete them.

All resources (independent domain names and SSL certificates) directly or indirectly associated with the group will be deleted. The operation will also unbind the external domain names from the subdomain name based on the CNAME resolution mode.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}

Table 4-22 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.

Request Parameters

Table 4-23 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 401

Table 4-24 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-25 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-26 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 412

Table 4-27 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500

Table 4-28 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3001",
  "error_msg" : "API group c77f5e81d9cb4424bf704ef2b0ac7600 does not exist"
}
```

Status code: 412

PreconditionFailed

```
{
  "error_code" : "APIG.3415",
  "error_msg" : "The API group cannot be deleted because it contains
APIs,id:47eaed4659db4e99ba2e1b642d5d1323"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
401	Unauthorized
403	Forbidden
404	Not Found
412	PreconditionFailed
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.1.4 Querying API Group Details

Function

This API is used to query the details of an API group.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}

Table 4-29 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.

Request Parameters

Table 4-30 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-31 Response body parameters

Parameter	Type	Description
id	String	ID.
name	String	API group name.
status	Integer	Status. 1: valid
sl_domain	String	Subdomain name that APIG automatically allocates to the API group.
register_time	String	Creation time.
update_time	String	Last modification time.
on_sell_status	Integer	Indicates whether the API group has been listed on KooGallery. 1: listed 2: not listed 3: under review Not supported currently.
url_domains	Array of UrlDomain objects	Independent domain names bound to the API group.
sl_domain_access_enabled	Boolean	Whether the debugging domain name is accessible. Options: true and false. Default: true
sl_domains	Array of strings	Automatically allocated subdomain names.

Parameter	Type	Description
remark	String	Description.
call_limits	Integer	Total number of times all APIs in the API group can be accessed. Consider the payload capacity of the backend service when setting this parameter. By default, there is no limit on the number of API calls. Currently, this parameter is not supported.
time_interval	Integer	Period of time for limiting the number of API calls. Currently, this parameter is not supported.
time_unit	String	Time unit for limiting the number of API calls. Currently, this parameter is not supported.
is_default	Integer	Indicates whether the API group is the default group.
version	String	Group version. • V1: global group • V2: application-level group This parameter is not supported currently.
roma_app_id	String	ID of the integration application to which the API group belongs. This parameter is required when the group version is V2. Currently, this parameter is not supported.
roma_app_name	String	Name of the integration application to which the API group belongs. Currently, this parameter is not supported.

Table 4-32 UrlDomain

Parameter	Type	Description
id	String	Domain ID.

Parameter	Type	Description
domain	String	Domain name.
cname_status	Integer	CNAME resolution status of the domain name. • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
min_ssl_version	String	Minimum SSL version. TLS 1.1 and TLS 1.2 are supported. Default: TLSv1.1
verified_client_certificate_enabled	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false
is_has_trusted_root_ca	Boolean	Whether a trusted root certificate (CA) exists. The value is true if trusted_root_ca exists in the bound certificate. Default: false

Parameter	Type	Description
ingress_http_port	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ingress_https_port	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ssl_infos	Array of SslInfo objects	SSL certificate list.

Table 4-33 SslInfo

Parameter	Type	Description
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2
type	String	Certificate scope: • instance • global Default: global

Status code: 400**Table 4-34** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-35** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-36** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-37** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-38** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "update_time" : "2020-07-31T06:55:55Z",
  "name" : "api_group_001",
  "on_sell_status" : 2,
  "remark" : "API group 1",
  "sl_domains" : [ "c77f5e81d9cb4424bf704ef2b0ac7600.apic.****.com",
    "c77f5e81d9cb4424bf704ef2b0ac7600.apic.****.cn" ],
  "sl_domain" : "c77f5e81d9cb4424bf704ef2b0ac7600.apic.****.com",
  "id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "register_time" : "2020-07-31T06:55:55Z",
  "status" : 1,
  "is_default" : 2,
  "sl_domain_access_enabled" : true
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.1.5 Querying API Groups

Function

This API is used to query the API group list.

You can query all API groups in your account as a tenant, or query API groups of all tenants using an administrator account.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/api-groups

Table 4-39 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-40 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
id	No	String	API group ID.
name	No	String	API group name.
precise_search	No	String	Parameter name for exact matching. Only API group names are supported.

Request Parameters

Table 4-41 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-42 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
groups	Array of ApiGroupInfo objects	API groups.

Table 4-43 ApiGroupInfo

Parameter	Type	Description
id	String	ID.
name	String	API group name.
status	Integer	Status. 1: valid
sl_domain	String	Subdomain name that APIG automatically allocates to the API group.
register_time	String	Creation time.
update_time	String	Last modification time.

Parameter	Type	Description
on_sell_status	Integer	Indicates whether the API group has been listed on KooGallery. • 1: listed • 2: not listed • 3: under review Not supported currently.
url_domains	Array of UrlDomain objects	Independent domain names bound to the API group.
sl_domain_access_enabled	Boolean	Whether the debugging domain name is accessible. Options: true and false. Default: true
sl_domains	Array of strings	Automatically allocated subdomain names.
remark	String	Description.
call_limits	Integer	Total number of times all APIs in the API group can be accessed. Consider the payload capacity of the backend service when setting this parameter. By default, there is no limit on the number of API calls. Currently, this parameter is not supported.
time_interval	Integer	Period of time for limiting the number of API calls. Currently, this parameter is not supported.
time_unit	String	Time unit for limiting the number of API calls. Currently, this parameter is not supported.
is_default	Integer	Indicates whether the API group is the default group.
version	String	Group version. • V1: global group • V2: application-level group This parameter is not supported currently.

Parameter	Type	Description
roma_app_id	String	ID of the integration application to which the API group belongs. This parameter is required when the group version is V2. Currently, this parameter is not supported.
roma_app_name	String	Name of the integration application to which the API group belongs. Currently, this parameter is not supported.

Table 4-44 UrlDomain

Parameter	Type	Description
id	String	Domain ID.
domain	String	Domain name.
cname_status	Integer	CNAME resolution status of the domain name. • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
min_ssl_version	String	Minimum SSL version. TLS 1.1 and TLS 1.2 are supported. Default: TLSv1.1
verified_client_certificate_enabled	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false
is_has_trusted_root_ca	Boolean	Whether a trusted root certificate (CA) exists. The value is true if trusted_root_ca exists in the bound certificate. Default: false

Parameter	Type	Description
ingress_http_port	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ingress_https_port	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ssl_infos	Array of SslInfo objects	SSL certificate list.

Table 4-45 SslInfo

Parameter	Type	Description
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2
type	String	Certificate scope: • instance • global Default: global

Status code: 400**Table 4-46** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-47** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-48** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-49** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 2,
  "size" : 2,
  "groups" : [ {
    "update_time" : "2020-07-31T06:55:55Z",
    "name" : "api_group_001",
    "on_sell_status" : 2,
    "remark" : "API group 1",
    "sl_domains" : [ "c77f5e81d9cb4424bf704ef2b0ac7600.apic.***.com",
"c77f5e81d9cb4424bf704ef2b0ac7600.apic.***.cn" ],
    "sl_domain" : "c77f5e81d9cb4424bf704ef2b0ac7600.apic.***.com",
    "id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
    "register_time" : "2020-07-31T06:55:55Z",
    "status" : 1,
    "is_default" : 2,
    "sl_domain_access_enabled" : true
  }, {
    "update_time" : "2020-06-24T15:29:42.421926Z",
    "name" : "api_group_002",
    "on_sell_status" : 2,
    "remark" : "API group 2",
    "sl_domain" : "02a8ab3cb2784de5a096852829671ae7.apic.***.com",
    "sl_domains" : [ "02a8ab3cb2784de5a096852829671ae7.apic.***.com",
"02a8ab3cb2784de5a096852829671ae7.apic.***.cn" ],
    "id" : "02a8ab3cb2784de5a096852829671ae7",
    "register_time" : "2020-06-24T15:29:42.421926Z",
    "status" : 1,
    "is_default" : 2,
    "sl_domain_access_enabled" : true
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.1.6 Verifying an API Group Name

Function

This API is used to check whether the API group name exists.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/api-groups/check

Table 4-50 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-51 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-52 Request body parameters

Parameter	Mandatory	Type	Description
group_name	Yes	String	Name of the API group to be verified.
roma_app_id	No	String	Integration application ID. This is not supported currently.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-53 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error description.

Status code: 401**Table 4-54** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-55** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-56** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-57** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

```
{  
  "group_name" : "ApiGroup_demo"  
}
```

Example Responses

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.3201",  
  "error_msg" : "The API group name already exists"  
}
```

Status code: 401

Unauthorized

```
{  
  "error_code" : "APIG.1002",  
  "error_msg" : "Incorrect token or token resolution failed"  
}
```

Status code: 403

Forbidden

```
{  
  "error_code" : "APIG.1005",  
  "error_msg" : "No permissions to request this method"  
}
```

Status code: 404

Not Found

```
{  
  "error_code" : "APIG.3030",  
  "error_msg" : "The instance does not exist;id:f0fa1789-3b76-433b-a787-9892951c620ec"  
}
```

Status code: 500

Internal Server Error

```
{  
  "error_code" : "APIG.9999",  
  "error_msg" : "System error"  
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.2 Environment Management

4.2.1 Creating an Environment

Function

API providers can publish an API in different environments, such as the development, test, and production environments.

API information, such as the version, request address, and even request message, varies depending on the environment in which an API is published. For example, v1.0 of an API is published in the production environment, v1.1 in the test environment, and v1.2 in the development environment.

APIG provides environment management, enabling you to access APIG in different scenarios at minimal costs.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/envs

Table 4-58 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-59 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-60 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Environment name, which can contain letters, digits, and underscores (_) and must start with a letter. Minimum: 3 Maximum: 64
remark	No	String	Description. Maximum: 255

Response Parameters

Status code: 201

Table 4-61 Response body parameters

Parameter	Type	Description
create_time	String	Creation time.
name	String	Environment name.
remark	String	Description.
id	String	Environment ID.

Status code: 400

Table 4-62 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-63** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-64** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-65** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Creating an environment

```
{
  "name" : "DEV",
  "remark" : "Development environment"
}
```


Example Responses

Status code: 201

Created

```
{
  "create_time" : "2020-07-31T06:41:43.511347628Z",
  "name" : "DEV",
  "remark" : "Development environment",
  "id" : "7a1ad0c350844ee69479b47df9a881cb"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.2.2 Modifying an Environment

Function

This API is used to modify the information about an environment. Only the name and remark attributes of an environment can be modified.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/envs/{env_id}

Table 4-66 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
env_id	Yes	String	Environment ID.

Request Parameters

Table 4-67 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-68 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Environment name, which can contain letters, digits, and underscores (_) and must start with a letter. Minimum: 3 Maximum: 64
remark	No	String	Description. Maximum: 255

Response Parameters

Status code: 200

Table 4-69 Response body parameters

Parameter	Type	Description
create_time	String	Creation time.
name	String	Environment name.
remark	String	Description.
id	String	Environment ID.

Status code: 400

Table 4-70 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-71 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 403**Table 4-72** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-73** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-74** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Modifying an environment

```
{
  "name" : "DEV",
  "remark" : "Development environment"
}
```

Example Responses

Status code: 200

OK

```
{
  "create_time": "2020-07-31T06:41:43Z",
  "name": "DEV",
  "remark": "Development environment",
  "id": "7a1ad0c350844ee69479b47df9a881cb"
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2012",
  "error_msg": "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3003",
  "error_msg": "Environment 7a1ad0c350844ee69479b47df9a881cb does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

Status Code	Description
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.2.3 Deleting an Environment

Function

This API is used to delete an environment.

This operation will cause the APIs published in the environment to become inaccessible to relevant apps and users. Ensure that you have notified users of the deletion, or confirm that the APIs can be removed from the deleted environment.

You cannot delete environments where APIs have been published.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/envs/{env_id}

Table 4-75 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
env_id	Yes	String	Environment ID.

Request Parameters

Table 4-76 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 401

Table 4-77 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-78 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-79 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-80** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 401**

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3003",
  "error_msg" : "Environment 7a1ad0c350844ee69479b47df9a881cb does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content

Status Code	Description
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.2.4 Querying Environments

Function

This API is used to query environments.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/envs

Table 4-81 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-82 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
name	No	String	Environment name.

Request Parameters

Table 4-83 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-84 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.

Parameter	Type	Description
envs	Array of EnvInfo objects	Environment list.

Table 4-85 EnvInfo

Parameter	Type	Description
create_time	String	Creation time.
name	String	Environment name.
remark	String	Description.
id	String	Environment ID.

Status code: 400**Table 4-86** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-87** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-88** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-89** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "total" : 2,
  "size" : 2,
  "envs" : [ {
    "create_time" : "2019-02-12T19:42:19.914989Z",
    "name" : "RELEASE",
    "remark" : "xxx",
    "id" : "DEFAULT_ENVIRONMENT_RELEASE_ID"
  }, {
    "create_time" : "2020-07-31T06:41:43Z",
    "name" : "DEV",
    "remark" : "Development environment",
    "id" : "7a1ad0c350844ee69479b47df9a881cb"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.3 Environment Variable Management

4.3.1 Creating a Variable

Function

Publishing an API in different environments may involve various variables, such as API service deployment address and request version.

You can define environment variables when creating an API. When the API is called, the environment variables will be replaced with the variable values to distinguish environments.

Environment variables are defined for an API group and apply to all APIs in the group.

 NOTE

1. Environment variable names must be unique for an API group in the same environment.
2. Environment variable names are case-sensitive. For example, ABC and abc are two different variables.
3. APIs that use environment variables cannot be debugged.
4. You must enclose an environment variable in number signs (#) so that it can be replaced with the actual value of the environment in which the API is published. For example, if the URL of an API is `https://#address#:8080` and the value of variable address is 192.168.1.5 in the RELEASE environment, the real URL of the API is `https://192.168.1.5:8080` after publishing.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/env-variables

Table 4-90 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-91 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-92 Request body parameters

Parameter	Mandatory	Type	Description
variable_value	Yes	String	The variable value can contain 1 to 255 characters. Only letters, digits, and special characters (_-/:.) are allowed.
env_id	Yes	String	Environment ID. Minimum: 1 Maximum: 65
group_id	Yes	String	API group ID. Minimum: 1 Maximum: 65
variable_name	Yes	String	Variable name, which can contain 3 to 32 characters, starting with a letter. Only letters, digits, hyphens (-), and underscores (_) are allowed. The variable name is equivalent to #Name# in an API definition. Characters between the number signs are case-sensitive. The variable name will be replaced with the variable value after API publication. NOTE Chinese characters must be in UTF-8 or Unicode format.

Response Parameters

Status code: 201

Table 4-93 Response body parameters

Parameter	Type	Description
variable_value	String	The variable value can contain 1 to 255 characters. Only letters, digits, and special characters (_-/:.) are allowed.
env_id	String	Environment ID. Minimum: 1 Maximum: 65

Parameter	Type	Description
group_id	String	API group ID. Minimum: 1 Maximum: 65
variable_name	String	Variable name, which can contain 3 to 32 characters, starting with a letter. Only letters, digits, hyphens (-), and underscores (_) are allowed. The variable name is equivalent to #Name# in an API definition. Characters between the number signs are case-sensitive. The variable name will be replaced with the variable value after API publication. NOTE Chinese characters must be in UTF-8 or Unicode format.
id	String	Environment variable ID.

Status code: 400**Table 4-94** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-95** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-96 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-97** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-98** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Creating an environment variable

```
{
  "variable_name": "address",
  "variable_value": "192.168.1.5",
  "env_id": "7a1ad0c350844ee69479b47df9a881cb",
  "group_id": "c77f5e81d9cb4424bf704ef2b0ac7600"
}
```

Example Responses

Status code: 201

Created

```
{
  "variable_value": "192.168.1.5",
  "env_id": "7a1ad0c350844ee69479b47df9a881cb",
  "group_id": "c77f5e81d9cb4424bf704ef2b0ac7600",
  "id": "25054838a624400bbf2267cf5b3a3f70",
  "variable_name": "address"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3003",
  "error_msg" : "The instance does not exist;id:f0fa1789-3b76-433b-a787-9892951c620ec"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.3.2 Deleting a Variable

Function

This API is used to delete an environment variable.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/env-variables/
{env_variable_id}

Table 4-99 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
env_variable_id	Yes	String	Environment variable ID.

Request Parameters

Table 4-100 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 401

Table 4-101 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-102 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-103 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-104 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3011",
  "error_msg" : "The environment variable does not exist, id: 25054838a624400bbf2267cf5b3a3f70"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.3.3 Querying Variable Details

Function

This API is used to query the details of an environment variable.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/env-variables/{env_variable_id}

Table 4-105 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
env_variable_id	Yes	String	Environment variable ID.

Request Parameters

Table 4-106 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-107 Response body parameters

Parameter	Type	Description
variable_value	String	The variable value can contain 1 to 255 characters. Only letters, digits, and special characters (_-/:.) are allowed.
env_id	String	Environment ID. Minimum: 1 Maximum: 65
group_id	String	API group ID. Minimum: 1 Maximum: 65
variable_name	String	Variable name, which can contain 3 to 32 characters, starting with a letter. Only letters, digits, hyphens (-), and underscores (_) are allowed. The variable name is equivalent to #Name# in an API definition. Characters between the number signs are case-sensitive. The variable name will be replaced with the variable value after API publication. NOTE Chinese characters must be in UTF-8 or Unicode format.
id	String	Environment variable ID.

Status code: 401**Table 4-108** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-109** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 404

Table 4-110 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-111 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "variable_value" : "192.168.1.5",
  "env_id" : "7a1ad0c350844ee69479b47df9a881cb",
  "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "id" : "25054838a624400bbf2267cf5b3a3f70",
  "variable_name" : "address"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden


```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3011",
  "error_msg" : "The environment variable does not exist, id: 25054838a624400bbf2267cf5b3a3f70"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.3.4 Querying Environment Variables

Function

This API is used to query all environment variables under an API group.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/env-variables

Table 4-112 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-113 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
group_id	Yes	String	API group ID.
env_id	No	String	Environment ID.
variable_name	No	String	Variable name.
precise_search	No	String	Parameter name (variable_name) for exact matching

Request Parameters

Table 4-114 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-115** Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
variables	Array of EnvVariableInfo objects	Environment variable list.

Table 4-116 EnvVariableInfo

Parameter	Type	Description
variable_value	String	The variable value can contain 1 to 255 characters. Only letters, digits, and special characters (_-/:) are allowed.
env_id	String	Environment ID. Minimum: 1 Maximum: 65
group_id	String	API group ID. Minimum: 1 Maximum: 65

Parameter	Type	Description
variable_name	String	Variable name, which can contain 3 to 32 characters, starting with a letter. Only letters, digits, hyphens (-), and underscores (_) are allowed. The variable name is equivalent to #Name# in an API definition. Characters between the number signs are case-sensitive. The variable name will be replaced with the variable value after API publication. NOTE Chinese characters must be in UTF-8 or Unicode format.
id	String	Environment variable ID.

Status code: 400**Table 4-117** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-118** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-119** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-120 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "variables" : [ {
    "variable_value" : "8080",
    "env_id" : "cca3616af3684b329064b2a631cb3eeb",
    "group_id" : "73c58022f20d495aa18885d718647f09",
    "id" : "09ab8135722440b9bf5d107f2a09d409",
    "variable_name" : "port"
  }, {
    "variable_value" : "192.168.1.5",
    "env_id" : "7a1ad0c350844ee69479b47df9a881cb",
    "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
    "id" : "25054838a624400bbf2267cf5b3a3f70",
    "variable_name" : "address"
  } ],
  "total" : 2,
  "size" : 2
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
}
```

```
{
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.3.5 Modifying a Variable

Function

This API is used to modify an environment variable. If an environment variable is referenced by the backend service address of an API, modifying the environment variable will publish all APIs that use the variable again.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/env-variables/{env_variable_id}

Table 4-121 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
env_variable_id	Yes	String	Environment variable ID.

Request Parameters

Table 4-122 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-123 Request body parameters

Parameter	Mandatory	Type	Description
variable_value	Yes	String	The variable value can contain 1 to 255 characters. Only letters, digits, and special characters (_-/:) are allowed.

Response Parameters

Status code: 200

Table 4-124 Response body parameters

Parameter	Type	Description
variable_value	String	The variable value can contain 1 to 255 characters. Only letters, digits, and special characters (_-/:) are allowed.
env_id	String	Environment ID. Minimum: 1 Maximum: 65

Parameter	Type	Description
group_id	String	API group ID. Minimum: 1 Maximum: 65
variable_name	String	Variable name, which can contain 3 to 32 characters, starting with a letter. Only letters, digits, hyphens (-), and underscores (_) are allowed. The variable name is equivalent to #Name# in an API definition. Characters between the number signs are case-sensitive. The variable name will be replaced with the variable value after API publication. NOTE Chinese characters must be in UTF-8 or Unicode format.
id	String	Environment variable ID.

Status code: 400**Table 4-125** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401**Table 4-126** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403

Table 4-127 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-128** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-129** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

```
{
  "variable_value" : "192.168.1.5"
}
```

Example Responses**Status code: 200**

OK

```
{
  "variable_value" : "192.168.1.5",
  "env_id" : "7a1ad0c350844ee69479b47df9a881cb",
  "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "id" : "25054838a624400bbf2267cf5b3a3f70",
  "variable_name" : "address"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
}
```

```
{
  "error_msg" : "Invalid parameter value,parameterName:variable_name"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3003",
  "error_msg" : "Environment 7a1ad0c350844ee69479b47df9a881cb does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.4 Request Throttling Policy Management

4.4.1 Creating a Request Throttling Policy

Function

After an API goes online, the system attaches a request throttling policy to it by default. The API provider can change the request throttling policy based on the service capabilities and load of the API.

A request throttling policy restricts the maximum number of times an API can be called within a specified period.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/throttles

Table 4-130 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-131 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-132 Request body parameters

Parameter	Mandatory	Type	Description
app_call_limits	No	Integer	Maximum number of times the API can be accessed by an app within the same period. The value of this parameter cannot exceed the user call limit. The maximum value is 2,147,483,647. Enter a positive integer.
name	Yes	String	Request throttling policy name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
time_unit	Yes	String	Time unit for limiting the number of API calls.
remark	No	String	Description of the request throttling policy, which can contain a maximum of 255 characters.
api_call_limits	Yes	Integer	Maximum number of times an API can be accessed within a specified period. The value of this parameter cannot exceed the default limit 200 TPS. You can change the default limit to meet service requirements. The maximum value is 2,147,483,647. Enter a positive integer.
type	No	Integer	Type of the request throttling policy. • 1: API-based, limiting the maximum number of times a single API bound to the policy can be called within the specified period. • 2: API-shared, limiting the maximum number of times all APIs bound to the policy can be called within the specified period.

Parameter	Mandatory	Type	Description
enable_adaptive_control	No	String	Indicates whether to enable dynamic request throttling. • TRUE • FALSE Currently, this parameter is not supported.
user_calls	No	Integer	Maximum number of times the API can be accessed by a user within the same period. The value of this parameter cannot exceed the Max. API Requests. The maximum value is 2,147,483,647. Enter a positive integer.
time_interval	Yes	Integer	Period of time for limiting the number of API calls. This parameter applies with each API call limit. The maximum value is 2,147,483,647. Enter a positive integer.
ip_call_limits	No	Integer	Maximum number of times the API can be accessed by an IP address within the same period. The value of this parameter cannot exceed the API call limit. The maximum value is 2,147,483,647. Enter a positive integer.

Response Parameters

Status code: 201

Table 4-133 Response body parameters

Parameter	Type	Description
app_call_limits	Integer	Maximum number of times the API can be accessed by an app within the same period. The value of this parameter cannot exceed the user call limit. The maximum value is 2,147,483,647. Enter a positive integer.

Parameter	Type	Description
name	String	Request throttling policy name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
time_unit	String	Time unit for limiting the number of API calls.
remark	String	Description of the request throttling policy, which can contain a maximum of 255 characters.
api_call_limits	Integer	Maximum number of times an API can be accessed within a specified period. The value of this parameter cannot exceed the default limit 200 TPS. You can change the default limit to meet service requirements. The maximum value is 2,147,483,647. Enter a positive integer.
type	Integer	Type of the request throttling policy. • 1: API-based, limiting the maximum number of times a single API bound to the policy can be called within the specified period. • 2: API-shared, limiting the maximum number of times all APIs bound to the policy can be called within the specified period.
enable_adaptive_control	String	Indicates whether to enable dynamic request throttling. • TRUE • FALSE Currently, this parameter is not supported.
user_call_limits	Integer	Maximum number of times the API can be accessed by a user within the same period. The value of this parameter cannot exceed the Max. API Requests. The maximum value is 2,147,483,647. Enter a positive integer.
time_interval	Integer	Period of time for limiting the number of API calls. This parameter applies with each API call limit. The maximum value is 2,147,483,647. Enter a positive integer.

Parameter	Type	Description
ip_call_limits	Integer	Maximum number of times the API can be accessed by an IP address within the same period. The value of this parameter cannot exceed the API call limit. The maximum value is 2,147,483,647. Enter a positive integer.
id	String	Request throttling policy ID.
bind_num	Integer	Number of APIs to which the request throttling policy has been bound.
is_inclu_special_throttle	Integer	Indicates whether an excluded request throttling configuration has been created. • 1: yes • 2: no
create_time	String	Creation time.

Status code: 400**Table 4-134** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-135** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-136 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-137** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Creating a request throttling policy (max. API requests: 800; max. user requests: 500; max. app requests: 300; max. IP address requests: 600; period: 1s)

```
{
  "api_call_limits" : 800,
  "app_call_limits" : 300,
  "enable_adaptive_control" : "FALSE",
  "ip_call_limits" : 600,
  "name" : "throttle_demo",
  "remark" : "Total: 800 calls/second; user: 500 calls/second; app: 300 calls/second; IP address: 600 calls/second",
  "time_interval" : 1,
  "time_unit" : "SECOND",
  "type" : 1,
  "user_call_limits" : 500
}
```

Example Responses

Status code: 201

Created

```
{
  "name" : "throttle_demo",
  "create_time" : "2020-07-31T08:44:02.205366118Z",
  "remark" : "Total: 800 calls/second; user: 500 calls/second; app: 300 calls/second; IP address: 600 calls/second",
  "type" : 1,
  "time_interval" : 1,
  "ip_call_limits" : 600,
  "app_call_limits" : 300,
  "time_unit" : "SECOND",
  "api_call_limits" : 800,
  "id" : "3437448ad06f4e0c91a224183116e965",
  "user_call_limits" : 500,
  "enable_adaptive_control" : "FALSE",
  "bind_num" : 0,
}
```



```
"is_inclu_special_throttle" : 2
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.4.2 Modifying a Request Throttling Policy

Function

This API is used to modify the information about a request throttling policy.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}

Table 4-138 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
throttle_id	Yes	String	Request throttling policy ID.

Request Parameters

Table 4-139 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-140 Request body parameters

Parameter	Mandatory	Type	Description
app_call_limits	No	Integer	Maximum number of times the API can be accessed by an app within the same period. The value of this parameter cannot exceed the user call limit. The maximum value is 2,147,483,647. Enter a positive integer.
name	Yes	String	Request throttling policy name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
time_unit	Yes	String	Time unit for limiting the number of API calls.
remark	No	String	Description of the request throttling policy, which can contain a maximum of 255 characters.
api_call_limits	Yes	Integer	Maximum number of times an API can be accessed within a specified period. The value of this parameter cannot exceed the default limit 200 TPS. You can change the default limit to meet service requirements. The maximum value is 2,147,483,647. Enter a positive integer.
type	No	Integer	Type of the request throttling policy. • 1: API-based, limiting the maximum number of times a single API bound to the policy can be called within the specified period. • 2: API-shared, limiting the maximum number of times all APIs bound to the policy can be called within the specified period.

Parameter	Mandatory	Type	Description
enable_adaptive_control	No	String	Indicates whether to enable dynamic request throttling. • TRUE • FALSE Currently, this parameter is not supported.
user_calls	No	Integer	Maximum number of times the API can be accessed by a user within the same period. The value of this parameter cannot exceed the Max. API Requests. The maximum value is 2,147,483,647. Enter a positive integer.
time_interval	Yes	Integer	Period of time for limiting the number of API calls. This parameter applies with each API call limit. The maximum value is 2,147,483,647. Enter a positive integer.
ip_call_limits	No	Integer	Maximum number of times the API can be accessed by an IP address within the same period. The value of this parameter cannot exceed the API call limit. The maximum value is 2,147,483,647. Enter a positive integer.

Response Parameters

Status code: 200

Table 4-141 Response body parameters

Parameter	Type	Description
app_call_limits	Integer	Maximum number of times the API can be accessed by an app within the same period. The value of this parameter cannot exceed the user call limit. The maximum value is 2,147,483,647. Enter a positive integer.

Parameter	Type	Description
name	String	Request throttling policy name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
time_unit	String	Time unit for limiting the number of API calls.
remark	String	Description of the request throttling policy, which can contain a maximum of 255 characters.
api_call_limits	Integer	Maximum number of times an API can be accessed within a specified period. The value of this parameter cannot exceed the default limit 200 TPS. You can change the default limit to meet service requirements. The maximum value is 2,147,483,647. Enter a positive integer.
type	Integer	Type of the request throttling policy. • 1: API-based, limiting the maximum number of times a single API bound to the policy can be called within the specified period. • 2: API-shared, limiting the maximum number of times all APIs bound to the policy can be called within the specified period.
enable_adaptive_control	String	Indicates whether to enable dynamic request throttling. • TRUE • FALSE Currently, this parameter is not supported.
user_call_limits	Integer	Maximum number of times the API can be accessed by a user within the same period. The value of this parameter cannot exceed the Max. API Requests. The maximum value is 2,147,483,647. Enter a positive integer.
time_interval	Integer	Period of time for limiting the number of API calls. This parameter applies with each API call limit. The maximum value is 2,147,483,647. Enter a positive integer.

Parameter	Type	Description
ip_call_limits	Integer	Maximum number of times the API can be accessed by an IP address within the same period. The value of this parameter cannot exceed the API call limit. The maximum value is 2,147,483,647. Enter a positive integer.
id	String	Request throttling policy ID.
bind_num	Integer	Number of APIs to which the request throttling policy has been bound.
is_inclu_special_throttle	Integer	Indicates whether an excluded request throttling configuration has been created. • 1: yes • 2: no
create_time	String	Creation time.

Status code: 400**Table 4-142** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-143** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-144 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-145** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-146** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Modifying a request throttling policy (max. API requests: 800; max. user requests: 500; max. app requests: 300; max. IP address requests: 600; period: 1s)

```
{
  "name" : "throttle_demo",
  "remark" : "Total: 800 calls/second; user: 500 calls/second; app: 300 calls/second; IP address: 600 calls/second",
  "type" : 1,
  "time_interval" : 1,
  "ip_call_limits" : 600,
  "app_call_limits" : 300,
  "time_unit" : "SECOND",
  "api_call_limits" : 800,
  "user_call_limits" : 500
}
```

Example Responses

Status code: 200

OK

```
{
  "name" : "throttle_demo",
```

```
"create_time" : "2020-07-31T08:44:02.205366118Z",
"remark" : "Total: 800 calls/second; user: 500 calls/second; app: 300 calls/second; IP address: 600 calls/second",
"type" : 1,
"time_interval" : 1,
"ip_call_limits" : 600,
"app_call_limits" : 300,
"time_unit" : "SECOND",
"api_call_limits" : 800,
"id" : "3437448ad06f4e0c91a224183116e965",
"user_call_limits" : 500,
"enable_adaptive_control" : "FALSE",
"bind_num" : 0,
"is_inclu_special_throttle" : 2
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3005",
  "error_msg" : "Request throttling policy 3437448ad06f4e0c91a224183116e965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```


Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.4.3 Deleting a Request Throttling Policy

Function

This API is used to delete a request throttling policy and all binding relationships between the policy and APIs.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}

Table 4-147 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
throttle_id	Yes	String	Request throttling policy ID.

Request Parameters

Table 4-148 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 401

Table 4-149 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-150 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-151 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-152** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 401**

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3005",
  "error_msg" : "Request throttling policy 3437448ad06f4e0c91a224183116e965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content

Status Code	Description
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.4.4 Querying Request Throttling Policies

Function

This API is used to query all the request throttling policies.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/throttles

Table 4-153 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-154 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
id	No	String	Request throttling policy ID.
name	No	String	Request throttling policy name.
precise_search	No	String	Parameter name (name) for exact matching.

Request Parameters

Table 4-155 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-156 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
throttles	Array of ThrottlesInfo objects	Request throttling policy list.

Table 4-157 ThrottlesInfo

Parameter	Type	Description
app_call_limits	Integer	Maximum number of times the API can be accessed by an app within the same period. The value of this parameter cannot exceed the user call limit. The maximum value is 2,147,483,647. Enter a positive integer.
name	String	Request throttling policy name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
time_unit	String	Time unit for limiting the number of API calls.
remark	String	Description of the request throttling policy, which can contain a maximum of 255 characters.
api_call_limits	Integer	Maximum number of times an API can be accessed within a specified period. The value of this parameter cannot exceed the default limit 200 TPS. You can change the default limit to meet service requirements. The maximum value is 2,147,483,647. Enter a positive integer.

Parameter	Type	Description
type	Integer	Type of the request throttling policy. • 1: API-based, limiting the maximum number of times a single API bound to the policy can be called within the specified period. • 2: API-shared, limiting the maximum number of times all APIs bound to the policy can be called within the specified period.
enable_adaptive_control	String	Indicates whether to enable dynamic request throttling. • TRUE • FALSE Currently, this parameter is not supported.
user_call_limits	Integer	Maximum number of times the API can be accessed by a user within the same period. The value of this parameter cannot exceed the Max. API Requests. The maximum value is 2,147,483,647. Enter a positive integer.
time_interval	Integer	Period of time for limiting the number of API calls. This parameter applies with each API call limit. The maximum value is 2,147,483,647. Enter a positive integer.
ip_call_limits	Integer	Maximum number of times the API can be accessed by an IP address within the same period. The value of this parameter cannot exceed the API call limit. The maximum value is 2,147,483,647. Enter a positive integer.
id	String	Request throttling policy ID.
bind_num	Integer	Number of APIs to which the request throttling policy has been bound.
is_inclu_special_throttle	Integer	Indicates whether an excluded request throttling configuration has been created. • 1: yes • 2: no
create_time	String	Creation time.

Status code: 400**Table 4-158** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-159** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-160** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-161** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "throttles" : [ {
    "name" : "throttle_demo",
    "create_time" : "2020-07-31T08:44:02.205366118Z",
    "remark" : "Total: 800 calls/second; user: 500 calls/second; app: 300 calls/second; IP address: 600 calls/second",
    "type" : 1,
    "time_interval" : 1,
    "ip_call_limits" : 600,
    "app_call_limits" : 300,
    "time_unit" : "SECOND",
    "api_call_limits" : 800,
    "id" : "3437448ad06f4e0c91a224183116e965",
    "user_call_limits" : 500,
    "enable_adaptive_control" : "FALSE",
    "bind_num" : 0,
    "is_inclu_special_throttle" : 2
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK

Status Code	Description
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.4.5 Querying Details of a Request Throttling Policy

Function

This API is used to query the details of a request throttling policy.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}

Table 4-162 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
throttle_id	Yes	String	Request throttling policy ID.

Request Parameters

Table 4-163 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-164** Response body parameters

Parameter	Type	Description
app_call_limits	Integer	Maximum number of times the API can be accessed by an app within the same period. The value of this parameter cannot exceed the user call limit. The maximum value is 2,147,483,647. Enter a positive integer.
name	String	Request throttling policy name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
time_unit	String	Time unit for limiting the number of API calls.
remark	String	Description of the request throttling policy, which can contain a maximum of 255 characters.
api_call_limits	Integer	Maximum number of times an API can be accessed within a specified period. The value of this parameter cannot exceed the default limit 200 TPS. You can change the default limit to meet service requirements. The maximum value is 2,147,483,647. Enter a positive integer.

Parameter	Type	Description
type	Integer	Type of the request throttling policy. • 1: API-based, limiting the maximum number of times a single API bound to the policy can be called within the specified period. • 2: API-shared, limiting the maximum number of times all APIs bound to the policy can be called within the specified period.
enable_adaptive_control	String	Indicates whether to enable dynamic request throttling. • TRUE • FALSE Currently, this parameter is not supported.
user_call_limits	Integer	Maximum number of times the API can be accessed by a user within the same period. The value of this parameter cannot exceed the Max. API Requests. The maximum value is 2,147,483,647. Enter a positive integer.
time_interval	Integer	Period of time for limiting the number of API calls. This parameter applies with each API call limit. The maximum value is 2,147,483,647. Enter a positive integer.
ip_call_limits	Integer	Maximum number of times the API can be accessed by an IP address within the same period. The value of this parameter cannot exceed the API call limit. The maximum value is 2,147,483,647. Enter a positive integer.
id	String	Request throttling policy ID.
bind_num	Integer	Number of APIs to which the request throttling policy has been bound.
is_inclu_special_throttle	Integer	Indicates whether an excluded request throttling configuration has been created. • 1: yes • 2: no
create_time	String	Creation time.

Status code: 401**Table 4-165** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-166** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-167** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-168** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "name" : "throttle_demo",
  "create_time" : "2020-07-31T08:44:02.205366118Z",
  "remark" : "Total: 800 calls/second; user: 500 calls/second; app: 300 calls/second; IP address: 600 calls/second",
  "type" : 1,
  "time_interval" : 1,
  "ip_call_limits" : 600,
  "app_call_limits" : 300,
  "time_unit" : "SECOND",
  "api_call_limits" : 800,
  "id" : "3437448ad06f4e0c91a224183116e965",
  "user_call_limits" : 500,
  "enable_adaptive_control" : "FALSE",
  "bind_num" : 0,
  "is_inclu_special_throttle" : 2
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3005",
  "error_msg" : "Request throttling policy 3437448ad06f4e0c91a224183116e965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.5 API Management

4.5.1 Creating an API

Function

This API is used to create an API. An API is an interface that encapsulates a set of service capabilities.

The definition of an API defines how the API is called by users and how APIG accesses the actual backend service requested by users. APIG supports four backend types: HTTP/HTTPS, gRPC, FunctionGraph, and Mock.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/apis

Table 4-169 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-170 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-171 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	API name. It can contain 3 to 255 characters, starting with a letter or digit. Only letters, digits, and these special characters are allowed: -_./:()
type	Yes	Integer	API type. 1: public API 2: private API
version	No	String	API version. Maximum: 16
req_protocol	Yes	String	API request protocol: - HTTP - HTTPS - BOTH: Both HTTP and HTTPS are supported. - GRPCS Default: HTTPS
req_method	Yes	String	API request method. If the request protocol is set to GRPC, the request method is fixed to POST.

Parameter	Mandatory	Type	Description
req_uri	Yes	String	Request address, which can contain request parameters enclosed with braces {}. For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. NOTE The address must comply with the URI specifications.
auth_type	Yes	String	API authentication mode. Options: • NONE • APP • IAM • AUTHORIZER: custom authentication. When auth_type is set to AUTHORIZER, the authorizer_id field is mandatory.
auth_opt	No	AuthOpt object	Security authentication parameter.
cors	No	Boolean	Indicates whether CORS is supported. • TRUE: supported • FALSE: not supported Default: false
trace_enabled	No	Boolean	Whether to enable tracing. By default, it is disabled. Default: false
sampling_strategy	No	String	Sampling policy. This parameter is mandatory when tracing is enabled. • RATE: sampling by percentage

Parameter	Mandatory	Type	Description
sampling_param	No	String	Sampling parameter. When sampling by percentage, the value of this parameter is an integer ranging from 0 to 100. The default value is 100, which indicates all requests are sampled. It is recommended that align the value with the backend sampling percentage. Default: 100 Minimum: 1 Maximum: 64
match_mode	No	String	API matching mode: - SWA: Prefix match - NORMAL: Exact match Default value: NORMAL
backend_type	Yes	String	Backend type. Options: - HTTP: web backend - FUNCTION: FunctionGraph backend. When backend_type is set to FUNCTION, the func_info field is mandatory. - MOCK: mock backend. When backend_type is set to MOCK, the mock_info field is mandatory. - GRPC: gRPC backend.
remark	No	String	API description. It cannot exceed 255 characters.
group_id	Yes	String	ID of the API group to which the API belongs.
body_remark	No	String	API request body, which can be an example request body, media type, or parameters. Ensure that the request body does not exceed 20,480 characters.

Parameter	Mandatory	Type	Description
result_normal_sample	No	String	Example response for a successful request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.
result_failure_sample	No	String	Example response for a failed request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.
authorizer_id	No	String	ID of the frontend custom authorizer
tags	No	Array of strings	Tag. Use letters, digits, and special characters (-*#%.:_) and start with a letter. By default, 10 tags are supported. To increase the quota, contact technical support to modify the API_TAG_NUM_LIMIT configuration. Minimum: 1 Maximum: 128
response_id	No	String	Group response ID.
roma_app_id	No	String	Integration application ID. Currently, this parameter is not supported.
domain_name	No	String	Custom domain name bound to the API. Currently, this parameter is not supported.
tag	No	String	Tag. This field will be deprecated. You can use the tags field instead.

Parameter	Mandatory	Type	Description
content_type	No	String	Request content type: application/json application/xml multipart/form-data text/plain
is_send_fg_body_base64	No	Boolean	Specifies whether to perform Base64 encoding on the body for interaction with FunctionGraph. The body does not need to be encoded using Base64 only when content_type is set to application/json. Application scenario: • Custom authentication • Bound circuit breaker plugin with FunctionGraph backend downgrade policy • APIs with FunctionGraph backend Default: true
mock_info	No	ApiMockCreate object	Mock backend details.
func_info	No	ApiFuncCreate object	FunctionGraph backend details.
req_params	No	Array of ReqParamBase objects	Request parameters. This is unavailable if the request protocol is set to GRPC.
backend_params	No	Array of BackendParamBase objects	Backend parameters. This is unavailable if the request protocol is set to GRPC.
policy_mocks	No	Array of ApiPolicyMockCreate objects	Mock backend policies.
policy_functions	No	Array of ApiPolicyFunctionCreate objects	FunctionGraph backend policies.
backend_api	No	BackendApiCreate object	Web backend details.

Parameter	Mandatory	Type	Description
policy_https	No	Array of ApiPolicyHttpCreate objects	Web backend policies.

Table 4-172 AuthOpt

Parameter	Mandatory	Type	Description
app_code_auth_type	No	String	Indicates whether AppCode authentication is enabled. This parameter is valid only if auth_type is set to App. The default value is DISABLE. - DISABLE: AppCode authentication is disabled. - HEADER: AppCode authentication is enabled and the AppCode is located in the header. Default: DISABLE

Table 4-173 ApiMockCreate

Parameter	Mandatory	Type	Description
remark	No	String	Description. It cannot exceed 255 characters.
result_content	No	String	Response.
version	No	String	Function version. It cannot exceed 64 characters.
authorizer_id	No	String	Backend custom authorizer ID.

Table 4-174 ApiFuncCreate

Parameter	Mandatory	Type	Description
function_urn	Yes	String	Function URN.
remark	No	String	Description. It cannot exceed 255 characters.

Parameter	Mandatory	Type	Description
invocation_type	Yes	String	Invocation mode. • async: asynchronous • sync: synchronous
network_type	Yes	String	Function network architecture. • V1: non-VPC • V2: VPC
version	No	String	Function version. If both a function alias URN and version are passed, only the alias URN will be used. Maximum: 64
alias_urn	No	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
timeout	Yes	Integer	Timeout allowed for APIG to request the backend service. If the function network architecture is set to V1, the maximum timeout is 60,000. If the network architecture is set to V2, the maximum timeout is 600,000 and can be modified by using the gateway parameter backend_timeout. Unit: ms. Minimum: 1
authorizer_id	No	String	Backend custom authorizer ID.
req_protocol	No	String	Backend request protocol of a function. The value can be HTTPS (default) or GRPCS (available when the frontend request protocol is GRPCS). Default: HTTPS

Table 4-175 ReqParamBase

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name. The parameter name can contain 1 to 32 characters and must start with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
type	Yes	String	Parameter type.
location	Yes	String	Parameter location.
default_value	No	String	Default value.
sample_value	No	String	Example value.
required	No	Integer	Indicates whether the parameter is required. 1: yes 2: no The value of this parameter is 1 if Location is set to PATH, and 2 if Location is set to another value.
valid_enable	No	Integer	Indicates whether validity check is enabled. 1: enabled 2: disabled Default: 2
remark	No	String	Description. It cannot exceed 255 characters.
enumerations	No	String	Enumerated value.
min_num	No	Integer	Minimum value. This parameter is valid when type is set to NUMBER.
max_num	No	Integer	Maximum value. This parameter is valid when type is set to NUMBER.
min_size	No	Integer	Minimum length. This parameter is valid when type is set to STRING.

Parameter	Mandatory	Type	Description
max_size	No	Integer	Maximum length. This parameter is valid when type is set to STRING.
regular	No	String	Regular expression validation rule. Currently, this parameter is not supported.
json_schema	No	String	JSON validation rule. Currently, this parameter is not supported.
pass_through	No	Integer	Indicates whether to transparently transfer the parameter. 1: yes 2: no
orchestrations	No	Array of strings	Request parameter orchestration rules are prioritized in the same sequence as the list. The none_value rule in a rule list has the highest priority. A maximum of one none_value rule can be bound. The default rule in a rule list has the lowest priority. A maximum of one default rule can be bound. The preprocessing orchestration rule cannot be used as the last orchestration rule except the default rule. Only one parameter of each API can be bound with unique orchestration rules. The number of orchestration rules that can be bound is limited by quota. For details, see "Notes and Constraints" in APIG Service Overview.

Table 4-176 ApiPolicyMockCreate

Parameter	Mandatory	Type	Description
result_content	No	String	Response.
effect_mode	Yes	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	Yes	String	Backend name. It must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_params	No	Array of BackendParamBase objects	Backend parameters. This is unavailable for the GRPC backend.
conditions	Yes	Array of ApiConditionBase objects	Policy conditions.
authorizer_id	No	String	Backend custom authorizer ID.

Table 4-177 ApiPolicyFunctionCreate

Parameter	Mandatory	Type	Description
function_urn	Yes	String	Function URN.
invocation_type	Yes	String	Invocation mode. • async: asynchronous • sync: synchronous
network_type	Yes	String	Function network architecture. • V1: non-VPC • V2: VPC
version	No	String	Function version. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored. Maximum: 64

Parameter	Mandatory	Type	Description
alias_urn	No	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
timeout	No	Integer	Timeout allowed for APIG to request the backend service. If the function network architecture is set to V1, the maximum timeout is 60,000. If the network architecture is set to V2, the maximum timeout is 600,000 and can be modified by using the gateway parameter backend_timeout. Unit: ms. Minimum: 1
req_protocol	No	String	Backend request protocol of a function. The value can be HTTPS (default) or GRPCS (available when the frontend request protocol is GRPCS). Default: HTTPS
effect_mode	Yes	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	Yes	String	Backend name. It must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_params	No	Array of BackendParamBase objects	Backend parameters. This is unavailable for the GRPC backend.
conditions	Yes	Array of ApiConditionBase objects	Policy conditions.
authorizer_id	No	String	Backend custom authorizer ID.

Table 4-178 BackendApiCreate

Parameter	Mandatory	Type	Description
authorizer_id	No	String	Backend custom authorizer ID.
url_domain	No	String	Address of the backend service. This parameter is required when no VPC channel is used. It consists of a domain name or IP address and a port number. Maximum length: 255 characters. It must be in the format "Host name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
req_protocol	Yes	String	Request protocol. You can select GRPC or GRPCS for the GRPC backend.
remark	No	String	Description. It cannot exceed 255 characters.
req_method	Yes	String	Request method. For the GRPC backend, the request method is fixed to POST.
version	No	String	Web backend version, which can contain a maximum of 16 characters.

Parameter	Mandatory	Type	Description
req_uri	Yes	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications. For the GRPC backend, the request address is fixed to /.
timeout	Yes	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms. Minimum: 1
enable_client_ssl	No	Boolean	Indicates whether to enable two-way authentication.
retry_count	No	String	Number of retry attempts to request the backend service. The default value is -1. The value ranges from -1 to 10. -1 indicates that idempotent APIs will retry once and non-idempotent APIs will not retry. POST and PATCH are non-idempotent. GET, HEAD, PUT, OPTIONS, and DELETE are idempotent. Default: -1

Parameter	Mandatory	Type	Description
enable_sm_channel	No	Boolean	Indicates whether to enable SM cryptographic algorithms. This feature is only available if the gateway supports the SM cryptographic algorithms.
vpc_channel_info	No	ApiBackendVpcReq object	VPC channel details. This parameter is required if vpc_channel_status is set to 1.
vpc_channel_status	No	Integer	Indicates whether to use a VPC channel. • 1: A VPC channel is used. • 2: No VPC channel is used.

Table 4-179 ApiPolicyHttpCreate

Parameter	Mandatory	Type	Description
url_domain	No	String	Endpoint of the policy backend. An endpoint consists of a domain name or IP address and a port number, with not more than 255 characters. It must be in the format "Domain name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
req_protocol	Yes	String	Request protocol. Options include HTTP, HTTPS, GRPC, or GRPCS. You can select GRPC or GRPCS for the GRPC backend.

Parameter	Mandatory	Type	Description
req_method	Yes	String	Request method. Options include GET, POST, PUT, DELETE, HEAD, PATCH, OPTIONS, and ANY. This is fixed to POST for the GRPC backend.
req_uri	Yes	String	Request address, which can contain request parameters enclosed with braces {}. For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications. For the GRPC backend, the request address is fixed to /.
timeout	No	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms. Minimum: 1

Parameter	Mandatory	Type	Description
retry_count	No	String	Number of retry attempts to request the backend service. The default value is -1. The value ranges from -1 to 10. -1 indicates that idempotent APIs will retry once and non-idempotent APIs will not retry. POST and PATCH are non-idempotent. GET, HEAD, PUT, OPTIONS, and DELETE are idempotent. Default: -1
enable_sm_channel	No	Boolean	Indicates whether to enable SM cryptographic algorithms. This feature is only available if the gateway supports the SM cryptographic algorithms.
effect_mode	Yes	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	Yes	String	Backend name. It must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_params	No	Array of BackendParamBase objects	Backend parameters. This is unavailable for the GRPC backend.
conditions	Yes	Array of ApiConditionBase objects	Policy conditions.
authorizer_id	No	String	Backend custom authorizer ID.
vpc_channel_info	No	ApiBackendVpcReq object	VPC channel details. This parameter is required if vpc_channel_status is set to 1.
vpc_channel_status	No	Integer	Indicates whether to use a VPC channel. • 1: A VPC channel is used. • 2: No VPC channel is used.

Table 4-180 BackendParamBase

Parameter	Mandatory	Type	Description
origin	Yes	String	Parameter type. • REQUEST: backend parameter • CONSTANT: constant parameter • SYSTEM: system parameter
name	Yes	String	Parameter name. The parameter name must start with a letter and can only contain letters, digits, hyphens (-), underscores (_), and periods (.). Minimum: 1 Maximum: 32
remark	No	String	Description, which can contain a maximum of 255 characters.
location	Yes	String	Parameter location. The value can be PATH, QUERY, or HEADER.

Parameter	Mandatory	Type	Description
value	Yes	String	Parameter value, which can contain a maximum of 255 characters. If the origin type is REQUEST, the value of this parameter is the parameter name in req_params. If the origin type is CONSTANT, the value is a constant. If the origin type is SYSTEM, the value is a system parameter name. System parameters include gateway parameters, frontend authentication parameters, and backend authentication parameters. You can set the frontend or backend authentication parameters after enabling custom frontend or backend authentication. The gateway parameters are as follows: • \$context.sourcelp: source IP address of the API caller. • \$context.stage: deployment environment in which the API is called. • \$context.apild: API ID. • \$context.appld: ID of the app used by the API caller. • \$context.requestId: request ID generated when the API is called. • \$context.serverAddr: address of the gateway server. • \$context.serverName: name of the gateway server. • \$context.handleTime: time when the API request is processed. • \$context.providerAppId: ID of the app used by the API

Parameter	Mandatory	Type	Description
			owner. This parameter is currently not supported. Frontend authentication parameter: prefixed with "\$context.authorizer.frontend.". For example, to return "aaa" upon successful custom authentication, set this parameter to "\$context.authorizer.frontend.aaa". Backend authentication parameter: prefixed with "\$context.authorizer.backend.". For example, to return "aaa" upon successful custom authentication, set this parameter to "\$context.authorizer.backend.aaa".

Table 4-181 ApiConditionBase

Parameter	Mandatory	Type	Description
req_param_name	No	String	Input parameter name. This parameter is required if the policy type is param.
sys_param_name	No	String	Name of a built-in gateway parameter. This parameter is required if the policy type is system. The following parameters are supported: • req_path: request path. For example, /a/b. • req_method: request method. For example, GET. • reqPath: request path, which is discarded. For example, /a/b. • reqMethod: request method, which is discarded. For example, GET.

Parameter	Mandatory	Type	Description
cookie_param_name	No	String	COOKIE parameter name. This parameter is required if the policy type is cookie. Minimum: 0 Maximum: 255
frontend_auth_orizer_param_name	No	String	System parameter: frontend authentication parameter name. This parameter is mandatory when the policy type is frontend_auth_orizer. The frontend authentication parameter name is prefixed with \$context.authorizer.frontend. For example, if the frontend authentication parameter name is user_name, the name with the prefix will be \$context.authorizer.frontend.user_name.
condition_type	No	String	Policy condition. • exact: Exact match • enum: Enumeration • pattern: Regular expression This parameter is required when the policy type is param, system, cookie, or frontend_auth_orizer.
condition_origin	Yes	String	Policy type • param: parameter • source: source IP address • system: system parameter - gateway built-in parameter • cookie: COOKIE parameter • frontend_auth_orizer: system parameter - frontend authentication parameter
condition_value	Yes	String	Policy value. Maximum: 1024

Parameter	Mandatory	Type	Description
mapped_parameter_name	No	String	Name of a parameter generated after orchestration. This parameter is mandatory when condition_origin is set to orchestration. The generated parameter name must exist in the orchestration rule bound to the API.
mapped_parameter_location	No	String	Location of a parameter generated after orchestration. This parameter is mandatory when condition_origin is set to orchestration. This location must exist in the orchestration rule bound to the API.

Table 4-182 ApiBackendVpcReq

Parameter	Mandatory	Type	Description
vpc_channel_proxy_host	No	String	Proxy host.
vpc_channel_id	Yes	String	VPC channel ID.

Response Parameters

Status code: 201

Table 4-183 Response body parameters

Parameter	Type	Description
name	String	API name. It can contain 3 to 255 characters, starting with a letter or digit. Only letters, digits, and these special characters are allowed: -_./:()
type	Integer	API type. 1: public API 2: private API
version	String	API version. Maximum: 16

Parameter	Type	Description
req_protocol	String	API request protocol: • HTTP • HTTPS • BOTH: Both HTTP and HTTPS are supported. • GRPCS Default: HTTPS
req_method	String	API request method. If the request protocol is set to GRPC, the request method is fixed to POST.
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. NOTE The address must comply with the URI specifications.
auth_type	String	API authentication mode. Options: • NONE • APP • IAM • AUTHORIZER: custom authentication. When auth_type is set to AUTHORIZER, the authorizer_id field is mandatory.
auth_opt	AuthOpt object	Security authentication parameter.
cors	Boolean	Indicates whether CORS is supported. • TRUE: supported • FALSE: not supported Default: false
trace_enabled	Boolean	Whether to enable tracing. By default, it is disabled. Default: false
sampling_strategy	String	Sampling policy. This parameter is mandatory when tracing is enabled. • RATE: sampling by percentage

Parameter	Type	Description
sampling_param	String	Sampling parameter. When sampling by percentage, the value of this parameter is an integer ranging from 0 to 100. The default value is 100, which indicates all requests are sampled. It is recommended that align the value with the backend sampling percentage. Default: 100 Minimum: 1 Maximum: 64
match_mode	String	API matching mode: - SWA: Prefix match - NORMAL: Exact match Default value: NORMAL
backend_type	String	Backend type. Options: - HTTP: web backend - FUNCTION: FunctionGraph backend. When backend_type is set to FUNCTION, the func_info field is mandatory. - MOCK: mock backend. When backend_type is set to MOCK, the mock_info field is mandatory. - GRPC: gRPC backend.
remark	String	API description. It cannot exceed 255 characters.
group_id	String	ID of the API group to which the API belongs.
body_remark	String	API request body, which can be an example request body, media type, or parameters. Ensure that the request body does not exceed 20,480 characters.
result_normal_sample	String	Example response for a successful request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.

Parameter	Type	Description
result_failure_sample	String	Example response for a failed request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.
authorizer_id	String	ID of the frontend custom authorizer
tags	Array of strings	Tag. Use letters, digits, and special characters (-*#%.:_) and start with a letter. By default, 10 tags are supported. To increase the quota, contact technical support to modify the API_TAG_NUM_LIMIT configuration. Minimum: 1 Maximum: 128
response_id	String	Group response ID.
roma_app_id	String	Integration application ID. Currently, this parameter is not supported.
domain_name	String	Custom domain name bound to the API. Currently, this parameter is not supported.
tag	String	Tag. This field will be deprecated. You can use the tags field instead.
content_type	String	Request content type: application/json application/xml multipart/form-data text/plain

Parameter	Type	Description
is_send_fg_body_base64	Boolean	Specifies whether to perform Base64 encoding on the body for interaction with FunctionGraph. The body does not need to be encoded using Base64 only when content_type is set to application/json. Application scenario: • Custom authentication • Bound circuit breaker plug-in with FunctionGraph backend downgrade policy • APIs with FunctionGraph backend Default: true
id	String	API ID.
status	Integer	App status. • 1: valid
arrange_necessary	Integer	Indicates whether to enable orchestration.
register_time	String	Time when the API is registered.
update_time	String	Time when the API was last modified.
group_name	String	Name of the API group to which the API belongs.
group_version	String	Version of the API group to which the API belongs. The default value is V1. Other versions are not supported. Default: V1
run_env_id	String	ID of the environment in which the API has been published. Separate multiple environment IDs with vertical bars ().
run_env_name	String	Name of the environment in which the API has been published. Separate multiple environment names with vertical bars ().
publish_id	String	Publication record ID. Separate multiple publication record IDs with vertical bars ().

Parameter	Type	Description
publish_time	String	Publication time. Separate the time of multiple publication records with vertical bars ().
roma_app_name	String	Name of the integration application to which the API belongs. Currently, this parameter is not supported.
ld_api_id	String	ID of the corresponding custom backend API. Currently, this parameter is not supported.
backend_api	BackendApi object	Web backend details.
api_group_info	ApiGroupCommonInfo object	API group information.
func_info	ApiFunc object	FunctionGraph backend details.
mock_info	ApiMock object	Mock backend details.
req_params	Array of ReqParam objects	Request parameters.
backend_params	Array of BackendParam objects	Backend parameters.
policy_functions	Array of ApiPolicyFunctionResp objects	FunctionGraph backend policies.
policy_mocks	Array of ApiPolicyMockResp objects	Mock backend policies.
policy_https	Array of ApiPolicyHttpResp objects	Web backend policies.

Table 4-184 AuthOpt

Parameter	Type	Description
app_code_auth_type	String	Indicates whether AppCode authentication is enabled. This parameter is valid only if auth_type is set to App. The default value is DISABLE. - DISABLE: AppCode authentication is disabled. - HEADER: AppCode authentication is enabled and the AppCode is located in the header. Default: DISABLE

Table 4-185 BackendApi

Parameter	Type	Description
authorizer_id	String	Backend custom authorizer ID.
url_domain	String	Address of the backend service. This parameter is required when no VPC channel is used. It consists of a domain name or IP address and a port number. Maximum length: 255 characters. It must be in the format "Host name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
req_protocol	String	Request protocol. You can select GRPC or GRPCS for the GRPC backend.
remark	String	Description. It cannot exceed 255 characters.
req_method	String	Request method. For the GRPC backend, the request method is fixed to POST.
version	String	Web backend version, which can contain a maximum of 16 characters.

Parameter	Type	Description
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications. For the GRPC backend, the request address is fixed to /.
timeout	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms. Minimum: 1
enable_client_ssl	Boolean	Indicates whether to enable two-way authentication.
retry_count	String	Number of retry attempts to request the backend service. The default value is -1. The value ranges from -1 to 10. -1 indicates that idempotent APIs will retry once and non-idempotent APIs will not retry. POST and PATCH are non-idempotent. GET, HEAD, PUT, OPTIONS, and DELETE are idempotent. Default: -1
enable_sm_channel	Boolean	Indicates whether to enable SM cryptographic algorithms. This feature is only available if the gateway supports the SM cryptographic algorithms.
id	String	ID.

Parameter	Type	Description
status	Integer	Backend service status. 1: valid
register_time	String	Registration time.
update_time	String	Update time.
vpc_channel_info	VpcInfo object	VPC channel details. This parameter is required if vpc_channel_status is set to 1.
vpc_channel_status	Integer	Indicates whether to use a VPC channel. 1: A VPC channel is used. 2: No VPC channel is used.

Table 4-186 ApiGroupCommonInfo

Parameter	Type	Description
id	String	ID.
name	String	API group name.
status	Integer	Status. 1: valid
sl_domain	String	Subdomain name that APIG automatically allocates to the API group.
register_time	String	Creation time.
update_time	String	Last modification time.
on_sell_status	Integer	Indicates whether the API group has been listed on KooGallery. 1: listed 2: not listed 3: under review Not supported currently.
url_domains	Array of UrlDomain objects	Independent domain names bound to the API group.
sl_domain_access_enabled	Boolean	Whether the debugging domain name is accessible. Options: true and false. Default: true

Table 4-187 UrlDomain

Parameter	Type	Description
id	String	Domain ID.
domain	String	Domain name.
cname_status	Integer	CNAME resolution status of the domain name. • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
min_ssl_version	String	Minimum SSL version. TLS 1.1 and TLS 1.2 are supported. Default: TLSv1.1
verified_client_certificate_enabled	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false
is_has_trusted_root_ca	Boolean	Whether a trusted root certificate (CA) exists. The value is true if trusted_root_ca exists in the bound certificate. Default: false

Parameter	Type	Description
ingress_http_port	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ingress_https_port	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ssl_infos	Array of SslInfo objects	SSL certificate list.

Table 4-188 SslInfo

Parameter	Type	Description
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2
type	String	Certificate scope: • instance • global Default: global

Table 4-189 ApiFunc

Parameter	Type	Description
function_urn	String	Function URN.
remark	String	Description. It cannot exceed 255 characters.
invocation_type	String	Invocation mode. • async: asynchronous • sync: synchronous
network_type	String	Function network architecture. • V1: non-VPC • V2: VPC
version	String	Function version. If both a function alias URN and version are passed, only the alias URN will be used. Maximum: 64
alias_urn	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.

Parameter	Type	Description
timeout	Integer	Timeout allowed for APIG to request the backend service. If the function network architecture is set to V1, the maximum timeout is 60,000. If the network architecture is set to V2, the maximum timeout is 600,000 and can be modified by using the gateway parameter backend_timeout. Unit: ms. Minimum: 1
authorizer_id	String	Backend custom authorizer ID.
req_protocol	String	Backend request protocol of a function. The value can be HTTPS (default) or GRPCS (available when the frontend request protocol is GRPCS). Default: HTTPS
id	String	ID.
register_time	String	Registration time.
status	Integer	Backend service status. • 1: valid
update_time	String	Update time.

Table 4-190 ApiMock

Parameter	Type	Description
remark	String	Description. It cannot exceed 255 characters.
result_content	String	Response.
version	String	Function version. It cannot exceed 64 characters.
authorizer_id	String	Backend custom authorizer ID.
id	String	ID.
register_time	String	Registration time.
status	Integer	Backend service status. • 1: valid
update_time	String	Update time.

Table 4-191 ReqParam

Parameter	Type	Description
name	String	Parameter name. The parameter name can contain 1 to 32 characters and must start with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
type	String	Parameter type.
location	String	Parameter location.
default_value	String	Default value.
sample_value	String	Example value.
required	Integer	Indicates whether the parameter is required. 1: yes 2: no The value of this parameter is 1 if Location is set to PATH, and 2 if Location is set to another value.
valid_enable	Integer	Indicates whether validity check is enabled. 1: enabled 2: disabled Default: 2
remark	String	Description. It cannot exceed 255 characters.
enumerations	String	Enumerated value.
min_num	Integer	Minimum value. This parameter is valid when type is set to NUMBER.
max_num	Integer	Maximum value. This parameter is valid when type is set to NUMBER.
min_size	Integer	Minimum length. This parameter is valid when type is set to STRING.
max_size	Integer	Maximum length. This parameter is valid when type is set to STRING.

Parameter	Type	Description
regular	String	Regular expression validation rule. Currently, this parameter is not supported.
json_schema	String	JSON validation rule. Currently, this parameter is not supported.
pass_through	Integer	Indicates whether to transparently transfer the parameter. 1: yes 2: no
orchestrations	Array of strings	Request parameter orchestration rules are prioritized in the same sequence as the list. The none_value rule in a rule list has the highest priority. A maximum of one none_value rule can be bound. The default rule in a rule list has the lowest priority. A maximum of one default rule can be bound. The preprocessing orchestration rule cannot be used as the last orchestration rule except the default rule. Only one parameter of each API can be bound with unique orchestration rules. The number of orchestration rules that can be bound is limited by quota. For details, see "Notes and Constraints" in APIG Service Overview.
id	String	Parameter ID.

Table 4-192 ApiPolicyFunctionResp

Parameter	Type	Description
function_urn	String	Function URN.
invocation_type	String	Invocation mode. • async: asynchronous • sync: synchronous

Parameter	Type	Description
network_type	String	Function network architecture. • V1: non-VPC • V2: VPC
version	String	Function version. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored. Maximum: 64
alias_urn	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
timeout	Integer	Timeout allowed for APIG to request the backend service. If the function network architecture is set to V1, the maximum timeout is 60,000. If the network architecture is set to V2, the maximum timeout is 600,000 and can be modified by using the gateway parameter backend_timeout. Unit: ms. Minimum: 1
req_protocol	String	Backend request protocol of a function. The value can be HTTPS (default) or GRPCS (available when the frontend request protocol is GRPCS). Default: HTTPS
id	String	ID.
effect_mode	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	String	Backend name, which must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64

Parameter	Type	Description
backend_params	Array of BackendParam objects	Backend parameters.
conditions	Array of CoditionResp objects	Policy conditions.
authorizer_id	String	Backend custom authorizer ID.

Table 4-193 ApiPolicyMockResp

Parameter	Type	Description
id	String	ID.
effect_mode	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	String	Backend name, which must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_params	Array of BackendParam objects	Backend parameters.
conditions	Array of CoditionResp objects	Policy conditions.
authorizer_id	String	Backend custom authorizer ID.
result_content	String	Response.

Table 4-194 ApiPolicyHttpResp

Parameter	Type	Description
id	String	ID.
effect_mode	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.

Parameter	Type	Description
name	String	Backend name, which must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_params	Array of BackendParam objects	Backend parameters.
conditions	Array of CoditionResp objects	Policy conditions.
authorizer_id	String	Backend custom authorizer ID.
url_domain	String	Endpoint of the policy backend. An endpoint consists of a domain name or IP address and a port number, with not more than 255 characters. It must be in the format "Domain name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
req_protocol	String	Request protocol. Options include HTTP, HTTPS, GRPC, or GRPCS. You can select GRPC or GRPCS for the GRPC backend.
req_method	String	Request method. Options include GET, POST, PUT, DELETE, HEAD, PATCH, OPTIONS, and ANY. This is fixed to POST for the GRPC backend.

Parameter	Type	Description
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications. For the GRPC backend, the request address is fixed to /.
timeout	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms. Minimum: 1
retry_count	String	Number of retry attempts to request the backend service. The default value is -1. The value ranges from -1 to 10. -1 indicates that idempotent APIs will retry once and non-idempotent APIs will not retry. POST and PATCH are non-idempotent. GET, HEAD, PUT, OPTIONS, and DELETE are idempotent. Default: -1
enable_sm_channel	Boolean	Indicates whether to enable SM cryptographic algorithms. This feature is only available if the gateway supports the SM cryptographic algorithms.
vpc_channel_info	VpcInfo object	VPC channel details. This parameter is required if vpc_channel_status is set to 1.

Parameter	Type	Description
vpc_channel_status	Integer	Indicates whether to use a VPC channel. • 1: A VPC channel is used. • 2: No VPC channel is used.

Table 4-195 BackendParam

Parameter	Type	Description
origin	String	Parameter type. • REQUEST: backend parameter • CONSTANT: constant parameter • SYSTEM: system parameter
name	String	Parameter name. The parameter name must start with a letter and can only contain letters, digits, hyphens (-), underscores (_), and periods (.). Minimum: 1 Maximum: 32
remark	String	Description, which can contain a maximum of 255 characters.
location	String	Parameter location. The value can be PATH, QUERY, or HEADER.

Parameter	Type	Description
value	String	Parameter value, which can contain a maximum of 255 characters. If the origin type is REQUEST, the value of this parameter is the parameter name in req_params. If the origin type is CONSTANT, the value is a constant. If the origin type is SYSTEM, the value is a system parameter name. System parameters include gateway parameters, frontend authentication parameters, and backend authentication parameters. You can set the frontend or backend authentication parameters after enabling custom frontend or backend authentication. The gateway parameters are as follows: • <code>\$context.sourceIp</code>: source IP address of the API caller. • <code>\$context.stage</code>: deployment environment in which the API is called. • <code>\$context.apid</code>: API ID. • <code>\$context.appId</code>: ID of the app used by the API caller. • <code>\$context.requestId</code>: request ID generated when the API is called. • <code>\$context.serverAddr</code>: address of the gateway server. • <code>\$context.serverName</code>: name of the gateway server. • <code>\$context.handleTime</code>: time when the API request is processed. • <code>\$context.providerAppId</code>: ID of the app used by the API owner. This parameter is currently not supported. Frontend authentication parameter: prefixed with <code>"\$context.authorizer.frontend."</code>. For example, to return "aaa" upon successful custom authentication, set this parameter to <code>"\$context.authorizer.frontend.aaa"</code>.

Parameter	Type	Description
		Backend authentication parameter: prefixed with "\$context.authorizer.backend.". For example, to return "aaa" upon successful custom authentication, set this parameter to "\$context.authorizer.backend.aaa".
id	String	Parameter ID.
req_param_id	String	Request parameter ID.

Table 4-196 CoditionResp

Parameter	Type	Description
req_param_name	String	Input parameter name. This parameter is required if the policy type is param.
sys_param_name	String	Name of a built-in gateway parameter. This parameter is required if the policy type is system. The following parameters are supported: - req_path: request path. For example, /a/b. - req_method: request method. For example, GET. - reqPath: request path, which is discarded. For example, /a/b. - reqMethod: request method, which is discarded. For example, GET.
cookie_param_name	String	COOKIE parameter name. This parameter is required if the policy type is cookie. Minimum: 0 Maximum: 255

Parameter	Type	Description
frontend_authorizer_param_name	String	System parameter: frontend authentication parameter name. This parameter is mandatory when the policy type is frontend_authorizer. The frontend authentication parameter name is prefixed with \$context.authorizer.frontend. For example, if the frontend authentication parameter name is user_name, the name with the prefix will be \$context.authorizer.frontend.user_name.
condition_type	String	Policy condition. • exact: Exact match • enum: Enumeration • pattern: Regular expression This parameter is required when the policy type is param, system, cookie, or frontend_authorizer.
condition_origin	String	Policy type • param: parameter • source: source IP address • system: system parameter - gateway built-in parameter • cookie: COOKIE parameter • frontend_authorizer: system parameter - frontend authentication parameter
condition_value	String	Policy value. Maximum: 1024
mapped_param_name	String	Name of a parameter generated after orchestration. This parameter is mandatory when condition_origin is set to orchestration. The generated parameter name must exist in the orchestration rule bound to the API.
mapped_param_location	String	Location of a parameter generated after orchestration. This parameter is mandatory when condition_origin is set to orchestration. This location must exist in the orchestration rule bound to the API.

Parameter	Type	Description
id	String	ID.
req_param_id	String	Input parameter ID.
req_param_location	String	Input parameter location.

Table 4-197 VpcInfo

Parameter	Type	Description
ecs_id	String	Cloud server ID.
ecs_name	String	Cloud server name.
cascade_flag	Boolean	Indicates whether to use the cascading mode. Currently, this parameter is not supported.
vpc_channel_proxy_host	String	Proxy host.
vpc_channel_id	String	VPC channel ID.
vpc_channel_port	Integer	VPC channel port.

Status code: 400**Table 4-198** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-199** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-200** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-201** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-202** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

- Creating a web backend API

```
{
  "group_id": "c77f5e81d9cb4424bf704ef2b0ac7600",
  "match_mode": "NORMAL",
  "name": "Api_http",
  "auth_type": "AUTHORIZER",
  "authorizer_id": "0d982c1ac3da493dae47627b6439fc5c",
  "backend_type": "HTTP",
  "backend_api": {
    "url_domain": "192.168.189.156:12346",
    "req_protocol": "HTTP",
    "req_method": "GET",
    "req_uri": "/test/benchmark",
    "timeout": 5000,
    "retry_count": "-1"
  },
  "req_protocol": "HTTPS",
  "req_uri": "/test/http",
  "remark": "Web backend API",
  "type": 1,
  "req_method": "GET",
  "result_normal_sample": "Example success response",
}
```

```
"result_failure_sample" : "Example failure response",
"tags" : [ "webApi" ],
"req_params" : [ {
  "name" : "query_demo",
  "location" : "QUERY",
  "type" : "STRING",
  "required" : 1
}, {
  "name" : "header-demo",
  "location" : "HEADER",
  "type" : "STRING",
  "required" : 2
} ],
"backend_params" : [ {
  "name" : "backHeader",
  "value" : "header-demo",
  "location" : "HEADER",
  "origin" : "REQUEST"
}, {
  "name" : "backQuery",
  "value" : "query_demo",
  "location" : "QUERY",
  "origin" : "REQUEST"
}, {
  "name" : "X-CONSTANT-HEADER",
  "value" : "demo",
  "location" : "HEADER",
  "origin" : "CONSTANT",
  "remark" : "constant_demo"
}, {
  "name" : "app-id",
  "value" : "$context.appld",
  "location" : "HEADER",
  "origin" : "SYSTEM",
  "remark" : "App ID of the API caller"
} ]
}
```

- Creating a gRPC backend API

```
{
  "group_id" : "12345abc9215b40bd84f4c469d56daebe",
  "match_mode" : "NORMAL",
  "name" : "Api_grpc",
  "auth_type" : "APP",
  "backend_type" : "GRPC",
  "backend_api" : {
    "req_protocol" : "GRPCS",
    "req_method" : "POST",
    "req_uri" : "/",
    "timeout" : 5000,
    "retry_count" : "-1",
    "enable_client_ssl" : false,
    "vpc_channel_status" : 1,
    "vpc_channel_info" : {
      "vpc_channel_id" : "abcd1234512345678aab9a2614a197ef4"
    }
  },
  "req_protocol" : "GRPCS",
  "req_uri" : "/test/grpc",
  "remark" : "GRPC backend API",
  "type" : 1,
  "req_method" : "POST",
  "tags" : [ "grpcApi" ],
  "cors" : false,
  "trace_enabled" : true,
  "sampling_strategy" : "RATE",
  "sampling_param" : "10",
  "auth_opt" : {
    "app_code_auth_type" : "DISABLE"
  }
}
```

```
}  
}
```

- Creating a FunctionGraph backend API

```
{  
  "group_id": "c77f5e81d9cb4424bf704ef2b0ac7600",  
  "match_mode": "NORMAL",  
  "name": "Api_function",  
  "auth_type": "APP",  
  "backend_type": "FUNCTION",  
  "func_info": {  
    "authorizer_id": "5b8cd3f06f004115aec69c58f57272c9",  
    "function_urn": "urn:fss:xx-  
xxx-7:73d69ae0cfcf460190522d06b60f05ad:function:default:auto_testfunc93749",  
    "invocation_type": "sync",  
    "network_type": "V1",  
    "timeout": 5000,  
    "version": "latest",  
    "alias_urn":  
    "urn:fss:region01:73d69ae0cfcf460190522d06b60f05ad:function:default:auto_testfunc93749:!a1"  
  },  
  "req_protocol": "HTTPS",  
  "req_uri": "/test/function",  
  "remark": "FunctionGraph backend API",  
  "type": 1,  
  "req_method": "GET",  
  "result_normal_sample": "Example success response",  
  "result_failure_sample": "Example failure response",  
  "tags": [ "functionApi" ]  
}
```

- Creating a Mock backend API

```
{  
  "group_id": "c77f5e81d9cb4424bf704ef2b0ac7600",  
  "match_mode": "SWA",  
  "name": "Api_mock",  
  "auth_type": "IAM",  
  "backend_type": "MOCK",  
  "mock_info": {  
    "result_content": "mock success"  
  },  
  "policy_mocks": [ {  
    "name": "Mock policy backend",  
    "effect_mode": "ANY",  
    "result_content": "mock policy success",  
    "conditions": [ {  
      "condition_origin": "source",  
      "condition_value": "1.0.1.0"  
    } ]  
  } ],  
  "req_protocol": "HTTPS",  
  "req_uri": "/test/mock",  
  "remark": "Mock backend API",  
  "type": 1,  
  "req_method": "GET",  
  "result_normal_sample": "Example success response",  
  "result_failure_sample": "Example failure response",  
  "tags": [ "mockApi" ]  
}
```

Example Responses

Status code: 201

Created

- Example 1

```
{
  "id": "5f918d104dc84480a75166ba99efff21",
  "tags": [ "webApi" ],
  "arrange_necessary": 2,
  "backend_type": "HTTP",
  "auth_type": "AUTHORIZER",
  "auth_opt": {
    "app_code_auth_type": "DISABLE"
  },
  "authorizer_id": "0d982c1ac3da493dae47627b6439fc5c",
  "backend_api": {
    "update_time": "2020-07-31T12:42:51.325312994Z",
    "vpc_channel_status": 2,
    "url_domain": "xxx.xxx.xxx.xxx:12346",
    "req_protocol": "HTTP",
    "id": "1ce8fda3586d4371bd83c955df37e102",
    "req_method": "GET",
    "register_time": "2020-07-31T12:42:51.325312721Z",
    "req_uri": "/benchmark",
    "timeout": 5000,
    "status": 1,
    "retry_count": "-1"
  },
  "cors": false,
  "status": 1,
  "group_name": "api_group_001",
  "group_id": "c77f5e81d9cb4424bf704ef2b0ac7600",
  "group_version": "V1",
  "response_id": "981e6c8f847f47199a9faf4409b751a5",
  "match_mode": "NORMAL",
  "name": "Api_http",
  "req_protocol": "HTTPS",
  "req_method": "GET",
  "req_uri": "/test/http",
  "type": 1,
  "result_normal_sample": "Example success response",
  "result_failure_sample": "Example failure response",
  "version": "V0.0.1",
  "register_time": "2020-07-31T12:42:51.314357035Z",
  "update_time": "2020-07-31T12:42:51.314357324Z",
  "remark": "Web backend API",
  "req_params": [ {
    "name": "query_demo",
    "location": "QUERY",
    "type": "STRING",
    "valid_enable": 2,
    "required": 1,
    "id": "57c8bf3c97ef40ee94eace95dff30014",
    "pass_through": 1
  }, {
    "name": "header-demo",
    "location": "HEADER",
    "type": "STRING",
    "valid_enable": 2,
    "required": 2,
    "id": "8d993be96980415faa6b1fb2ebd647e0",
    "pass_through": 1
  } ],
  "backend_params": [ {
    "name": "backHeader",
    "value": "header-demo",
    "location": "HEADER",
    "origin": "REQUEST",
    "id": "709f0ea376b44aaf907aaaa37d8cce92",
    "req_param_id": "8d993be96980415faa6b1fb2ebd647e0"
  }, {
    "name": "backQuery",
    "value": "query_demo",
    "location": "QUERY",
```

```
"origin" : "REQUEST",
"id" : "2f152d0fb54445039158d29c2a4f69ee",
"req_param_id" : "57c8bf3c97ef40ee94eace95dff30014"
}, {
  "name" : "X-CONSTANT-HEADER",
  "value" : "demo",
  "location" : "HEADER",
  "origin" : "CONSTANT",
  "remark" : "constant_demo",
  "id" : "20142102c6aa4f3c97d5fd6ef4010ac2"
}, {
  "name" : "app-id",
  "value" : "$context.appld",
  "location" : "HEADER",
  "origin" : "SYSTEM",
  "remark" : "App ID of the API caller",
  "id" : "a1349c61016e4d999ca783a50bfee2b"
}]
}
```

- Example 2

```
{
  "id" : "8789c9367rd1439rf869c23cc0d1ef22",
  "tags" : [ "grpcApi" ],
  "arrange_necessary" : 2,
  "backend_type" : "GRPC",
  "auth_type" : "APP",
  "auth_opt" : {
    "app_code_auth_type" : "DISABLE"
  },
  "backend_api" : {
    "update_time" : "2023-08-29T09:05:17.652404554Z",
    "vpc_channel_status" : 1,
    "vpc_channel_info" : {
      "cascade_flag" : false,
      "vpc_channel_id" : "abcd1234512345678aab9a2614a197ef4",
      "vpc_channel_port" : 0
    },
    "url_domain" : "abcd1234512345678aab9a2614a197ef4",
    "req_protocol" : "GRPCS",
    "id" : "c0123456789d421cb83a396955bd48d0",
    "req_method" : "POST",
    "register_time" : "2023-08-29T09:05:17.652404454Z",
    "req_uri" : "/",
    "timeout" : 5000,
    "enable_client_ssl" : false,
    "retry_count" : "-1",
    "status" : 1
  },
  "cors" : false,
  "trace_enabled" : true,
  "sampling_strategy" : "RATE",
  "sampling_param" : "10",
  "status" : 1,
  "group_name" : "api_group_001",
  "group_id" : "12345abc9215b40bd84f4c469d56daebe",
  "group_version" : "V1",
  "response_id" : "ef21ec8c7df94d72a44f9rf1461c5f62",
  "match_mode" : "NORMAL",
  "name" : "Api_grpc",
  "req_protocol" : "GRPCS",
  "req_method" : "POST",
  "req_uri" : "/test/grpc",
  "type" : 1,
  "version" : "V0.0.1",
  "register_time" : "2023-08-29T09:05:17.647533939Z",
  "update_time" : "2023-08-29T09:05:17.647534036Z",
  "remark" : "GRPC backend API",
  "api_group_info" : {
    "id" : "12345abc9215b40bd84f4c469d56daebe",
```



```
"name" : "api_group_001",
"status" : 1,
"sl_domain" : "12345abc9215b40bd84f4c469d56daebe.apic.region-1.example.com",
"register_time" : "2023-08-29T08:38:21Z",
"update_time" : "2023-08-29T08:38:21Z",
"on_sell_status" : 2,
"sl_domain_access_enabled" : true
}
}
```

- Example 3

```
{
  "id" : "abd9c4b2ff974888b0ba79be7e6b2763",
  "arrange_necessary" : 2,
  "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "group_name" : "api_group_001",
  "group_version" : "V1",
  "match_mode" : "NORMAL",
  "name" : "Api_function",
  "auth_type" : "APP",
  "auth_opt" : {
    "auth_code_auth_type" : "DISABLE"
  },
  "backend_type" : "FUNCTION",
  "func_info" : {
    "id" : "c0740524cd4c40e3801a7afe5375f8b0",
    "authorizer_id" : "5b8cd3f06f004115aec69c58f57272c9",
    "function_urn" : "urn:fss:xxx-7:73d69ae0cfcf460190522d06b60f05ad:function:default:auto_testfunc93749",
    "invocation_type" : "sync",
    "network_type" : "V1",
    "timeout" : 5000,
    "version" : "latest",
    "alias_urn" : "urn:fss:region01:73d69ae0cfcf460190522d06b60f05ad:function:default:auto_testfunc00000:1a1",
    "register_time" : "2020-08-02T15:36:19.897262803Z",
    "update_time" : "2020-08-02T15:36:19.897262993Z",
    "status" : 1
  },
  "cors" : false,
  "req_protocol" : "HTTPS",
  "req_uri" : "/test/function",
  "remark" : "FunctionGraph backend API",
  "type" : 1,
  "version" : "V0.0.1",
  "status" : 1,
  "req_method" : "GET",
  "result_normal_sample" : "Example success response",
  "result_failure_sample" : "Example failure response",
  "tags" : [ "functionApi" ],
  "register_time" : "2020-08-02T15:36:19.892012381Z",
  "update_time" : "2020-08-02T15:36:19.892012627Z"
}
```

- Example 4

```
{
  "id" : "3a955b791bd24b1c9cd94c745f8d1aad",
  "arrange_necessary" : 2,
  "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "group_name" : "api_group_001",
  "group_version" : "V1",
  "match_mode" : "SWA",
  "name" : "Api_mock",
  "auth_type" : "IAM",
  "auth_opt" : {
    "auth_code_auth_type" : "DISABLE"
  },
  "backend_type" : "MOCK",
  "mock_info" : {
    "id" : "e74bbc75825c4c38ae84ccab6bdc6175",

```

```
"result_content" : "mock success",
"update_time" : "2020-08-02T15:56:52.301790686Z",
"register_time" : "2020-08-02T15:56:52.301790367Z"
},
"policy_mocks" : [ {
  "name" : "Mock policy backend",
  "id" : "1cb05173a4c84b7d996e30145cce3c7d",
  "effect_mode" : "ANY",
  "result_content" : "mock policy success",
  "conditions" : [ {
    "condition_origin" : "source",
    "condition_value" : "1.0.1.0",
    "id" : "8650b3a94e7344df8251658d8aee1f6d"
  } ]
} ],
"cors" : false,
"req_protocol" : "HTTPS",
"req_uri" : "/test/mock",
"remark" : "Mock backend API",
"type" : 1,
"version" : "V0.0.1",
"req_method" : "GET",
"result_normal_sample" : "Example success response",
"result_failure_sample" : "Example failure response",
"tags" : [ "mockApi" ],
"register_time" : "2020-08-02T15:56:52.286099413Z",
"update_time" : "2020-08-02T15:56:52.286099715Z",
"status" : 1
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3019",
  "error_msg" : "The function URN does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.5.2 Modifying an API

Function

This API is used to modify the information about an API, including its backend information.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/apis/{api_id}

Table 4-203 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Parameter	Mandatory	Type	Description
api_id	Yes	String	API ID.

Request Parameters

Table 4-204 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-205 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	API name. It can contain 3 to 255 characters, starting with a letter or digit. Only letters, digits, and these special characters are allowed: -_./:()
type	Yes	Integer	API type. 1: public API 2: private API
version	No	String	API version. Maximum: 16
req_protocol	Yes	String	API request protocol: - HTTP - HTTPS - BOTH: Both HTTP and HTTPS are supported. - GRPCS Default: HTTPS
req_method	Yes	String	API request method. If the request protocol is set to GRPC, the request method is fixed to POST.

Parameter	Mandatory	Type	Description
req_uri	Yes	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. NOTE The address must comply with the URI specifications.
auth_type	Yes	String	API authentication mode. Options: • NONE • APP • IAM • AUTHORIZER: custom authentication. When auth_type is set to AUTHORIZER, the authorizer_id field is mandatory.
auth_opt	No	AuthOpt object	Security authentication parameter.
cors	No	Boolean	Indicates whether CORS is supported. • TRUE: supported • FALSE: not supported Default: false
trace_enabled	No	Boolean	Whether to enable tracing. By default, it is disabled. Default: false
sampling_strategy	No	String	Sampling policy. This parameter is mandatory when tracing is enabled. • RATE: sampling by percentage

Parameter	Mandatory	Type	Description
sampling_param	No	String	Sampling parameter. When sampling by percentage, the value of this parameter is an integer ranging from 0 to 100. The default value is 100, which indicates all requests are sampled. It is recommended that align the value with the backend sampling percentage. Default: 100 Minimum: 1 Maximum: 64
match_mode	No	String	API matching mode: - SWA: Prefix match - NORMAL: Exact match Default value: NORMAL
backend_type	Yes	String	Backend type. Options: - HTTP: web backend - FUNCTION: FunctionGraph backend. When backend_type is set to FUNCTION, the func_info field is mandatory. - MOCK: mock backend. When backend_type is set to MOCK, the mock_info field is mandatory. - GRPC: gRPC backend.
remark	No	String	API description. It cannot exceed 255 characters.
group_id	Yes	String	ID of the API group to which the API belongs.
body_remark	No	String	API request body, which can be an example request body, media type, or parameters. Ensure that the request body does not exceed 20,480 characters.

Parameter	Mandatory	Type	Description
result_normal_sample	No	String	Example response for a successful request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.
result_failure_sample	No	String	Example response for a failed request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.
authorizer_id	No	String	ID of the frontend custom authorizer
tags	No	Array of strings	Tag. Use letters, digits, and special characters (-*#%.:_) and start with a letter. By default, 10 tags are supported. To increase the quota, contact technical support to modify the API_TAG_NUM_LIMIT configuration. Minimum: 1 Maximum: 128
response_id	No	String	Group response ID.
roma_app_id	No	String	Integration application ID. Currently, this parameter is not supported.
domain_name	No	String	Custom domain name bound to the API. Currently, this parameter is not supported.
tag	No	String	Tag. This field will be deprecated. You can use the tags field instead.

Parameter	Mandatory	Type	Description
content_type	No	String	Request content type: application/json application/xml multipart/form-data text/plain
is_send_fg_body_base64	No	Boolean	Specifies whether to perform Base64 encoding on the body for interaction with FunctionGraph. The body does not need to be encoded using Base64 only when content_type is set to application/json. Application scenario: • Custom authentication • Bound circuit breaker plugin with FunctionGraph backend downgrade policy • APIs with FunctionGraph backend Default: true
mock_info	No	ApiMockCreate object	Mock backend details.
func_info	No	ApiFuncCreate object	FunctionGraph backend details.
req_params	No	Array of ReqParamBase objects	Request parameters. This is unavailable if the request protocol is set to GRPC.
backend_params	No	Array of BackendParamBase objects	Backend parameters. This is unavailable if the request protocol is set to GRPC.
policy_mocks	No	Array of ApiPolicyMockCreate objects	Mock backend policies.
policy_functions	No	Array of ApiPolicyFunctionCreate objects	FunctionGraph backend policies.
backend_api	No	BackendApiCreate object	Web backend details.

Parameter	Mandatory	Type	Description
policy_https	No	Array of ApiPolicyHttpCreate objects	Web backend policies.

Table 4-206 AuthOpt

Parameter	Mandatory	Type	Description
app_code_auth_type	No	String	Indicates whether AppCode authentication is enabled. This parameter is valid only if auth_type is set to App. The default value is DISABLE. - DISABLE: AppCode authentication is disabled. - HEADER: AppCode authentication is enabled and the AppCode is located in the header. Default: DISABLE

Table 4-207 ApiMockCreate

Parameter	Mandatory	Type	Description
remark	No	String	Description. It cannot exceed 255 characters.
result_content	No	String	Response.
version	No	String	Function version. It cannot exceed 64 characters.
authorizer_id	No	String	Backend custom authorizer ID.

Table 4-208 ApiFuncCreate

Parameter	Mandatory	Type	Description
function_urn	Yes	String	Function URN.
remark	No	String	Description. It cannot exceed 255 characters.

Parameter	Mandatory	Type	Description
invocation_type	Yes	String	Invocation mode. • async: asynchronous • sync: synchronous
network_type	Yes	String	Function network architecture. • V1: non-VPC • V2: VPC
version	No	String	Function version. If both a function alias URN and version are passed, only the alias URN will be used. Maximum: 64
alias_urn	No	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
timeout	Yes	Integer	Timeout allowed for APIG to request the backend service. If the function network architecture is set to V1, the maximum timeout is 60,000. If the network architecture is set to V2, the maximum timeout is 600,000 and can be modified by using the gateway parameter backend_timeout. Unit: ms. Minimum: 1
authorizer_id	No	String	Backend custom authorizer ID.
req_protocol	No	String	Backend request protocol of a function. The value can be HTTPS (default) or GRPCS (available when the frontend request protocol is GRPCS). Default: HTTPS

Table 4-209 ReqParamBase

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name. The parameter name can contain 1 to 32 characters and must start with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
type	Yes	String	Parameter type.
location	Yes	String	Parameter location.
default_value	No	String	Default value.
sample_value	No	String	Example value.
required	No	Integer	Indicates whether the parameter is required. 1: yes 2: no The value of this parameter is 1 if Location is set to PATH, and 2 if Location is set to another value.
valid_enable	No	Integer	Indicates whether validity check is enabled. 1: enabled 2: disabled Default: 2
remark	No	String	Description. It cannot exceed 255 characters.
enumerations	No	String	Enumerated value.
min_num	No	Integer	Minimum value. This parameter is valid when type is set to NUMBER.
max_num	No	Integer	Maximum value. This parameter is valid when type is set to NUMBER.
min_size	No	Integer	Minimum length. This parameter is valid when type is set to STRING.

Parameter	Mandatory	Type	Description
max_size	No	Integer	Maximum length. This parameter is valid when type is set to STRING.
regular	No	String	Regular expression validation rule. Currently, this parameter is not supported.
json_schema	No	String	JSON validation rule. Currently, this parameter is not supported.
pass_through	No	Integer	Indicates whether to transparently transfer the parameter. 1: yes 2: no
orchestrations	No	Array of strings	Request parameter orchestration rules are prioritized in the same sequence as the list. The none_value rule in a rule list has the highest priority. A maximum of one none_value rule can be bound. The default rule in a rule list has the lowest priority. A maximum of one default rule can be bound. The preprocessing orchestration rule cannot be used as the last orchestration rule except the default rule. Only one parameter of each API can be bound with unique orchestration rules. The number of orchestration rules that can be bound is limited by quota. For details, see "Notes and Constraints" in APIG Service Overview.

Table 4-210 ApiPolicyMockCreate

Parameter	Mandatory	Type	Description
result_content	No	String	Response.
effect_mode	Yes	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	Yes	String	Backend name. It must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_parameters	No	Array of BackendParameterBase objects	Backend parameters. This is unavailable for the GRPC backend.
conditions	Yes	Array of ApiConditionBase objects	Policy conditions.
authorizer_id	No	String	Backend custom authorizer ID.

Table 4-211 ApiPolicyFunctionCreate

Parameter	Mandatory	Type	Description
function_urn	Yes	String	Function URN.
invocation_type	Yes	String	Invocation mode. • async: asynchronous • sync: synchronous
network_type	Yes	String	Function network architecture. • V1: non-VPC • V2: VPC
version	No	String	Function version. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored. Maximum: 64

Parameter	Mandatory	Type	Description
alias_urn	No	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
timeout	No	Integer	Timeout allowed for APIG to request the backend service. If the function network architecture is set to V1, the maximum timeout is 60,000. If the network architecture is set to V2, the maximum timeout is 600,000 and can be modified by using the gateway parameter backend_timeout. Unit: ms. Minimum: 1
req_protocol	No	String	Backend request protocol of a function. The value can be HTTPS (default) or GRPCS (available when the frontend request protocol is GRPCS). Default: HTTPS
effect_mode	Yes	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	Yes	String	Backend name. It must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_params	No	Array of BackendParamBase objects	Backend parameters. This is unavailable for the GRPC backend.
conditions	Yes	Array of ApiConditionBase objects	Policy conditions.
authorizer_id	No	String	Backend custom authorizer ID.

Table 4-212 BackendApiCreate

Parameter	Mandatory	Type	Description
authorizer_id	No	String	Backend custom authorizer ID.
url_domain	No	String	Address of the backend service. This parameter is required when no VPC channel is used. It consists of a domain name or IP address and a port number. Maximum length: 255 characters. It must be in the format "Host name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
req_protocol	Yes	String	Request protocol. You can select GRPC or GRPCS for the GRPC backend.
remark	No	String	Description. It cannot exceed 255 characters.
req_method	Yes	String	Request method. For the GRPC backend, the request method is fixed to POST.
version	No	String	Web backend version, which can contain a maximum of 16 characters.

Parameter	Mandatory	Type	Description
req_uri	Yes	String	Request address, which can contain request parameters enclosed with braces {}. For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications. For the GRPC backend, the request address is fixed to /.
timeout	Yes	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms. Minimum: 1
enable_client_ssl	No	Boolean	Indicates whether to enable two-way authentication.
retry_count	No	String	Number of retry attempts to request the backend service. The default value is -1. The value ranges from -1 to 10. -1 indicates that idempotent APIs will retry once and non-idempotent APIs will not retry. POST and PATCH are non-idempotent. GET, HEAD, PUT, OPTIONS, and DELETE are idempotent. Default: -1

Parameter	Mandatory	Type	Description
enable_sm_channel	No	Boolean	Indicates whether to enable SM cryptographic algorithms. This feature is only available if the gateway supports the SM cryptographic algorithms.
vpc_channel_info	No	ApiBackendVpcReq object	VPC channel details. This parameter is required if vpc_channel_status is set to 1.
vpc_channel_status	No	Integer	Indicates whether to use a VPC channel. 1: A VPC channel is used. 2: No VPC channel is used.

Table 4-213 ApiPolicyHttpCreate

Parameter	Mandatory	Type	Description
url_domain	No	String	Endpoint of the policy backend. An endpoint consists of a domain name or IP address and a port number, with not more than 255 characters. It must be in the format "Domain name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
req_protocol	Yes	String	Request protocol. Options include HTTP, HTTPS, GRPC, or GRPCS. You can select GRPC or GRPCS for the GRPC backend.

Parameter	Mandatory	Type	Description
req_method	Yes	String	Request method. Options include GET, POST, PUT, DELETE, HEAD, PATCH, OPTIONS, and ANY. This is fixed to POST for the GRPC backend.
req_uri	Yes	String	Request address, which can contain request parameters enclosed with braces {}. For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications. For the GRPC backend, the request address is fixed to /.
timeout	No	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms. Minimum: 1

Parameter	Mandatory	Type	Description
retry_count	No	String	Number of retry attempts to request the backend service. The default value is -1. The value ranges from -1 to 10. -1 indicates that idempotent APIs will retry once and non-idempotent APIs will not retry. POST and PATCH are non-idempotent. GET, HEAD, PUT, OPTIONS, and DELETE are idempotent. Default: -1
enable_sm_channel	No	Boolean	Indicates whether to enable SM cryptographic algorithms. This feature is only available if the gateway supports the SM cryptographic algorithms.
effect_mode	Yes	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	Yes	String	Backend name. It must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_params	No	Array of BackendParamBase objects	Backend parameters. This is unavailable for the GRPC backend.
conditions	Yes	Array of ApiConditionBase objects	Policy conditions.
authorizer_id	No	String	Backend custom authorizer ID.
vpc_channel_info	No	ApiBackendVpcReq object	VPC channel details. This parameter is required if vpc_channel_status is set to 1.
vpc_channel_status	No	Integer	Indicates whether to use a VPC channel. • 1: A VPC channel is used. • 2: No VPC channel is used.

Table 4-214 BackendParamBase

Parameter	Mandatory	Type	Description
origin	Yes	String	Parameter type. • REQUEST: backend parameter • CONSTANT: constant parameter • SYSTEM: system parameter
name	Yes	String	Parameter name. The parameter name must start with a letter and can only contain letters, digits, hyphens (-), underscores (_), and periods (.). Minimum: 1 Maximum: 32
remark	No	String	Description, which can contain a maximum of 255 characters.
location	Yes	String	Parameter location. The value can be PATH, QUERY, or HEADER.

Parameter	Mandatory	Type	Description
value	Yes	String	Parameter value, which can contain a maximum of 255 characters. If the origin type is REQUEST, the value of this parameter is the parameter name in req_params. If the origin type is CONSTANT, the value is a constant. If the origin type is SYSTEM, the value is a system parameter name. System parameters include gateway parameters, frontend authentication parameters, and backend authentication parameters. You can set the frontend or backend authentication parameters after enabling custom frontend or backend authentication. The gateway parameters are as follows: • \$context.sourcelp: source IP address of the API caller. • \$context.stage: deployment environment in which the API is called. • \$context.apild: API ID. • \$context.appld: ID of the app used by the API caller. • \$context.requestId: request ID generated when the API is called. • \$context.serverAddr: address of the gateway server. • \$context.serverName: name of the gateway server. • \$context.handleTime: time when the API request is processed. • \$context.providerAppId: ID of the app used by the API

Parameter	Mandatory	Type	Description
			owner. This parameter is currently not supported. Frontend authentication parameter: prefixed with "\$context.authorizer.frontend.". For example, to return "aaa" upon successful custom authentication, set this parameter to "\$context.authorizer.frontend.aaa". Backend authentication parameter: prefixed with "\$context.authorizer.backend.". For example, to return "aaa" upon successful custom authentication, set this parameter to "\$context.authorizer.backend.aaa".

Table 4-215 ApiConditionBase

Parameter	Mandatory	Type	Description
req_param_name	No	String	Input parameter name. This parameter is required if the policy type is param.
sys_param_name	No	String	Name of a built-in gateway parameter. This parameter is required if the policy type is system. The following parameters are supported: • req_path: request path. For example, /a/b. • req_method: request method. For example, GET. • reqPath: request path, which is discarded. For example, /a/b. • reqMethod: request method, which is discarded. For example, GET.

Parameter	Mandatory	Type	Description
cookie_param_name	No	String	COOKIE parameter name. This parameter is required if the policy type is cookie. Minimum: 0 Maximum: 255
frontend_auth_orizer_param_name	No	String	System parameter: frontend authentication parameter name. This parameter is mandatory when the policy type is frontend_auth_orizer. The frontend authentication parameter name is prefixed with \$context.authorizer.frontend. For example, if the frontend authentication parameter name is user_name, the name with the prefix will be \$context.authorizer.frontend.user_name.
condition_type	No	String	Policy condition. • exact: Exact match • enum: Enumeration • pattern: Regular expression This parameter is required when the policy type is param, system, cookie, or frontend_auth_orizer.
condition_origin	Yes	String	Policy type • param: parameter • source: source IP address • system: system parameter - gateway built-in parameter • cookie: COOKIE parameter • frontend_auth_orizer: system parameter - frontend authentication parameter
condition_value	Yes	String	Policy value. Maximum: 1024

Parameter	Mandatory	Type	Description
mapped_parameter_name	No	String	Name of a parameter generated after orchestration. This parameter is mandatory when condition_origin is set to orchestration. The generated parameter name must exist in the orchestration rule bound to the API.
mapped_parameter_location	No	String	Location of a parameter generated after orchestration. This parameter is mandatory when condition_origin is set to orchestration. This location must exist in the orchestration rule bound to the API.

Table 4-216 ApiBackendVpcReq

Parameter	Mandatory	Type	Description
vpc_channel_proxy_host	No	String	Proxy host.
vpc_channel_id	Yes	String	VPC channel ID.

Response Parameters

Status code: 200

Table 4-217 Response body parameters

Parameter	Type	Description
name	String	API name. It can contain 3 to 255 characters, starting with a letter or digit. Only letters, digits, and these special characters are allowed: -_./:()
type	Integer	API type. 1: public API 2: private API
version	String	API version. Maximum: 16

Parameter	Type	Description
req_protocol	String	API request protocol: • HTTP • HTTPS • BOTH: Both HTTP and HTTPS are supported. • GRPCS Default: HTTPS
req_method	String	API request method. If the request protocol is set to GRPC, the request method is fixed to POST.
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. NOTE The address must comply with the URI specifications.
auth_type	String	API authentication mode. Options: • NONE • APP • IAM • AUTHORIZER: custom authentication. When auth_type is set to AUTHORIZER, the authorizer_id field is mandatory.
auth_opt	AuthOpt object	Security authentication parameter.
cors	Boolean	Indicates whether CORS is supported. • TRUE: supported • FALSE: not supported Default: false
trace_enabled	Boolean	Whether to enable tracing. By default, it is disabled. Default: false
sampling_strategy	String	Sampling policy. This parameter is mandatory when tracing is enabled. • RATE: sampling by percentage

Parameter	Type	Description
sampling_param	String	Sampling parameter. When sampling by percentage, the value of this parameter is an integer ranging from 0 to 100. The default value is 100, which indicates all requests are sampled. It is recommended that align the value with the backend sampling percentage. Default: 100 Minimum: 1 Maximum: 64
match_mode	String	API matching mode: - SWA: Prefix match - NORMAL: Exact match Default value: NORMAL
backend_type	String	Backend type. Options: - HTTP: web backend - FUNCTION: FunctionGraph backend. When backend_type is set to FUNCTION, the func_info field is mandatory. - MOCK: mock backend. When backend_type is set to MOCK, the mock_info field is mandatory. - GRPC: gRPC backend.
remark	String	API description. It cannot exceed 255 characters.
group_id	String	ID of the API group to which the API belongs.
body_remark	String	API request body, which can be an example request body, media type, or parameters. Ensure that the request body does not exceed 20,480 characters.
result_normal_sample	String	Example response for a successful request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.

Parameter	Type	Description
result_failure_sample	String	Example response for a failed request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.
authorizer_id	String	ID of the frontend custom authorizer
tags	Array of strings	Tag. Use letters, digits, and special characters (-*#%.:_) and start with a letter. By default, 10 tags are supported. To increase the quota, contact technical support to modify the API_TAG_NUM_LIMIT configuration. Minimum: 1 Maximum: 128
response_id	String	Group response ID.
roma_app_id	String	Integration application ID. Currently, this parameter is not supported.
domain_name	String	Custom domain name bound to the API. Currently, this parameter is not supported.
tag	String	Tag. This field will be deprecated. You can use the tags field instead.
content_type	String	Request content type: application/json application/xml multipart/form-data text/plain

Parameter	Type	Description
is_send_fg_body_base64	Boolean	Specifies whether to perform Base64 encoding on the body for interaction with FunctionGraph. The body does not need to be encoded using Base64 only when content_type is set to application/json. Application scenario: • Custom authentication • Bound circuit breaker plug-in with FunctionGraph backend downgrade policy • APIs with FunctionGraph backend Default: true
id	String	API ID.
status	Integer	App status. • 1: valid
arrange_necessary	Integer	Indicates whether to enable orchestration.
register_time	String	Time when the API is registered.
update_time	String	Time when the API was last modified.
group_name	String	Name of the API group to which the API belongs.
group_version	String	Version of the API group to which the API belongs. The default value is V1. Other versions are not supported. Default: V1
run_env_id	String	ID of the environment in which the API has been published. Separate multiple environment IDs with vertical bars ().
run_env_name	String	Name of the environment in which the API has been published. Separate multiple environment names with vertical bars ().
publish_id	String	Publication record ID. Separate multiple publication record IDs with vertical bars ().

Parameter	Type	Description
publish_time	String	Publication time. Separate the time of multiple publication records with vertical bars ().
roma_app_name	String	Name of the integration application to which the API belongs. Currently, this parameter is not supported.
ld_api_id	String	ID of the corresponding custom backend API. Currently, this parameter is not supported.
backend_api	BackendApi object	Web backend details.
api_group_info	ApiGroupCommonInfo object	API group information.
func_info	ApiFunc object	FunctionGraph backend details.
mock_info	ApiMock object	Mock backend details.
req_params	Array of ReqParam objects	Request parameters.
backend_params	Array of BackendParam objects	Backend parameters.
policy_functions	Array of ApiPolicyFunctionResp objects	FunctionGraph backend policies.
policy_mock	Array of ApiPolicyMockResp objects	Mock backend policies.
policy_https	Array of ApiPolicyHttpResp objects	Web backend policies.

Table 4-218 AuthOpt

Parameter	Type	Description
app_code_auth_type	String	Indicates whether AppCode authentication is enabled. This parameter is valid only if auth_type is set to App. The default value is DISABLE. • DISABLE: AppCode authentication is disabled. • HEADER: AppCode authentication is enabled and the AppCode is located in the header. Default: DISABLE

Table 4-219 BackendApi

Parameter	Type	Description
authorizer_id	String	Backend custom authorizer ID.
url_domain	String	Address of the backend service. This parameter is required when no VPC channel is used. It consists of a domain name or IP address and a port number. Maximum length: 255 characters. It must be in the format "Host name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
req_protocol	String	Request protocol. You can select GRPC or GRPCS for the GRPC backend.
remark	String	Description. It cannot exceed 255 characters.
req_method	String	Request method. For the GRPC backend, the request method is fixed to POST.
version	String	Web backend version, which can contain a maximum of 16 characters.

Parameter	Type	Description
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications. For the GRPC backend, the request address is fixed to /.
timeout	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms. Minimum: 1
enable_client_ssl	Boolean	Indicates whether to enable two-way authentication.
retry_count	String	Number of retry attempts to request the backend service. The default value is -1. The value ranges from -1 to 10. -1 indicates that idempotent APIs will retry once and non-idempotent APIs will not retry. POST and PATCH are non-idempotent. GET, HEAD, PUT, OPTIONS, and DELETE are idempotent. Default: -1
enable_sm_channel	Boolean	Indicates whether to enable SM cryptographic algorithms. This feature is only available if the gateway supports the SM cryptographic algorithms.
id	String	ID.

Parameter	Type	Description
status	Integer	Backend service status. 1: valid
register_time	String	Registration time.
update_time	String	Update time.
vpc_channel_info	VpcInfo object	VPC channel details. This parameter is required if vpc_channel_status is set to 1.
vpc_channel_status	Integer	Indicates whether to use a VPC channel. 1: A VPC channel is used. 2: No VPC channel is used.

Table 4-220 ApiGroupCommonInfo

Parameter	Type	Description
id	String	ID.
name	String	API group name.
status	Integer	Status. 1: valid
sl_domain	String	Subdomain name that APIG automatically allocates to the API group.
register_time	String	Creation time.
update_time	String	Last modification time.
on_sell_status	Integer	Indicates whether the API group has been listed on KooGallery. 1: listed 2: not listed 3: under review Not supported currently.
url_domains	Array of UrlDomain objects	Independent domain names bound to the API group.
sl_domain_access_enabled	Boolean	Whether the debugging domain name is accessible. Options: true and false. Default: true

Table 4-221 UrlDomain

Parameter	Type	Description
id	String	Domain ID.
domain	String	Domain name.
cname_status	Integer	CNAME resolution status of the domain name. • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
min_ssl_version	String	Minimum SSL version. TLS 1.1 and TLS 1.2 are supported. Default: TLSv1.1
verified_client_certificate_enabled	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false
is_has_trusted_root_ca	Boolean	Whether a trusted root certificate (CA) exists. The value is true if trusted_root_ca exists in the bound certificate. Default: false

Parameter	Type	Description
ingress_http_port	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ingress_https_port	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ssl_infos	Array of SslInfo objects	SSL certificate list.

Table 4-222 SslInfo

Parameter	Type	Description
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2
type	String	Certificate scope: • instance • global Default: global

Table 4-223 ApiFunc

Parameter	Type	Description
function_urn	String	Function URN.
remark	String	Description. It cannot exceed 255 characters.
invocation_type	String	Invocation mode. • async: asynchronous • sync: synchronous
network_type	String	Function network architecture. • V1: non-VPC • V2: VPC
version	String	Function version. If both a function alias URN and version are passed, only the alias URN will be used. Maximum: 64
alias_urn	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.

Parameter	Type	Description
timeout	Integer	Timeout allowed for APIG to request the backend service. If the function network architecture is set to V1, the maximum timeout is 60,000. If the network architecture is set to V2, the maximum timeout is 600,000 and can be modified by using the gateway parameter backend_timeout. Unit: ms. Minimum: 1
authorizer_id	String	Backend custom authorizer ID.
req_protocol	String	Backend request protocol of a function. The value can be HTTPS (default) or GRPCS (available when the frontend request protocol is GRPCS). Default: HTTPS
id	String	ID.
register_time	String	Registration time.
status	Integer	Backend service status. • 1: valid
update_time	String	Update time.

Table 4-224 ApiMock

Parameter	Type	Description
remark	String	Description. It cannot exceed 255 characters.
result_content	String	Response.
version	String	Function version. It cannot exceed 64 characters.
authorizer_id	String	Backend custom authorizer ID.
id	String	ID.
register_time	String	Registration time.
status	Integer	Backend service status. • 1: valid
update_time	String	Update time.

Table 4-225 ReqParam

Parameter	Type	Description
name	String	Parameter name. The parameter name can contain 1 to 32 characters and must start with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
type	String	Parameter type.
location	String	Parameter location.
default_value	String	Default value.
sample_value	String	Example value.
required	Integer	Indicates whether the parameter is required. 1: yes 2: no The value of this parameter is 1 if Location is set to PATH, and 2 if Location is set to another value.
valid_enable	Integer	Indicates whether validity check is enabled. 1: enabled 2: disabled Default: 2
remark	String	Description. It cannot exceed 255 characters.
enumerations	String	Enumerated value.
min_num	Integer	Minimum value. This parameter is valid when type is set to NUMBER.
max_num	Integer	Maximum value. This parameter is valid when type is set to NUMBER.
min_size	Integer	Minimum length. This parameter is valid when type is set to STRING.
max_size	Integer	Maximum length. This parameter is valid when type is set to STRING.

Parameter	Type	Description
regular	String	Regular expression validation rule. Currently, this parameter is not supported.
json_schema	String	JSON validation rule. Currently, this parameter is not supported.
pass_through	Integer	Indicates whether to transparently transfer the parameter. 1: yes 2: no
orchestrations	Array of strings	Request parameter orchestration rules are prioritized in the same sequence as the list. The none_value rule in a rule list has the highest priority. A maximum of one none_value rule can be bound. The default rule in a rule list has the lowest priority. A maximum of one default rule can be bound. The preprocessing orchestration rule cannot be used as the last orchestration rule except the default rule. Only one parameter of each API can be bound with unique orchestration rules. The number of orchestration rules that can be bound is limited by quota. For details, see "Notes and Constraints" in APIG Service Overview.
id	String	Parameter ID.

Table 4-226 ApiPolicyFunctionResp

Parameter	Type	Description
function_urn	String	Function URN.
invocation_type	String	Invocation mode. • async: asynchronous • sync: synchronous

Parameter	Type	Description
network_type	String	Function network architecture. • V1: non-VPC • V2: VPC
version	String	Function version. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored. Maximum: 64
alias_urn	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
timeout	Integer	Timeout allowed for APIG to request the backend service. If the function network architecture is set to V1, the maximum timeout is 60,000. If the network architecture is set to V2, the maximum timeout is 600,000 and can be modified by using the gateway parameter backend_timeout. Unit: ms. Minimum: 1
req_protocol	String	Backend request protocol of a function. The value can be HTTPS (default) or GRPCS (available when the frontend request protocol is GRPCS). Default: HTTPS
id	String	ID.
effect_mode	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	String	Backend name, which must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64

Parameter	Type	Description
backend_params	Array of BackendParam objects	Backend parameters.
conditions	Array of CoditionResp objects	Policy conditions.
authorizer_id	String	Backend custom authorizer ID.

Table 4-227 ApiPolicyMockResp

Parameter	Type	Description
id	String	ID.
effect_mode	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	String	Backend name, which must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_params	Array of BackendParam objects	Backend parameters.
conditions	Array of CoditionResp objects	Policy conditions.
authorizer_id	String	Backend custom authorizer ID.
result_content	String	Response.

Table 4-228 ApiPolicyHttpResp

Parameter	Type	Description
id	String	ID.
effect_mode	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.

Parameter	Type	Description
name	String	Backend name, which must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_params	Array of BackendParam objects	Backend parameters.
conditions	Array of CoditionResp objects	Policy conditions.
authorizer_id	String	Backend custom authorizer ID.
url_domain	String	Endpoint of the policy backend. An endpoint consists of a domain name or IP address and a port number, with not more than 255 characters. It must be in the format "Domain name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
req_protocol	String	Request protocol. Options include HTTP, HTTPS, GRPC, or GRPCS. You can select GRPC or GRPCS for the GRPC backend.
req_method	String	Request method. Options include GET, POST, PUT, DELETE, HEAD, PATCH, OPTIONS, and ANY. This is fixed to POST for the GRPC backend.

Parameter	Type	Description
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications. For the GRPC backend, the request address is fixed to /.
timeout	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms. Minimum: 1
retry_count	String	Number of retry attempts to request the backend service. The default value is -1. The value ranges from -1 to 10. -1 indicates that idempotent APIs will retry once and non-idempotent APIs will not retry. POST and PATCH are non-idempotent. GET, HEAD, PUT, OPTIONS, and DELETE are idempotent. Default: -1
enable_sm_channel	Boolean	Indicates whether to enable SM cryptographic algorithms. This feature is only available if the gateway supports the SM cryptographic algorithms.
vpc_channel_info	VpcInfo object	VPC channel details. This parameter is required if vpc_channel_status is set to 1.

Parameter	Type	Description
vpc_channel_status	Integer	Indicates whether to use a VPC channel. • 1: A VPC channel is used. • 2: No VPC channel is used.

Table 4-229 BackendParam

Parameter	Type	Description
origin	String	Parameter type. • REQUEST: backend parameter • CONSTANT: constant parameter • SYSTEM: system parameter
name	String	Parameter name. The parameter name must start with a letter and can only contain letters, digits, hyphens (-), underscores (_), and periods (.). Minimum: 1 Maximum: 32
remark	String	Description, which can contain a maximum of 255 characters.
location	String	Parameter location. The value can be PATH, QUERY, or HEADER.

Parameter	Type	Description
value	String	Parameter value, which can contain a maximum of 255 characters. If the origin type is REQUEST, the value of this parameter is the parameter name in req_params. If the origin type is CONSTANT, the value is a constant. If the origin type is SYSTEM, the value is a system parameter name. System parameters include gateway parameters, frontend authentication parameters, and backend authentication parameters. You can set the frontend or backend authentication parameters after enabling custom frontend or backend authentication. The gateway parameters are as follows: • \$context.sourceIp: source IP address of the API caller. • \$context.stage: deployment environment in which the API is called. • \$context.apid: API ID. • \$context.appId: ID of the app used by the API caller. • \$context.requestId: request ID generated when the API is called. • \$context.serverAddr: address of the gateway server. • \$context.serverName: name of the gateway server. • \$context.handleTime: time when the API request is processed. • \$context.providerAppId: ID of the app used by the API owner. This parameter is currently not supported. Frontend authentication parameter: prefixed with "\$context.authorizer.frontend.". For example, to return "aaa" upon successful custom authentication, set this parameter to "\$context.authorizer.frontend.aaa".

Parameter	Type	Description
		Backend authentication parameter: prefixed with "\$context.authorizer.backend.". For example, to return "aaa" upon successful custom authentication, set this parameter to "\$context.authorizer.backend.aaa".
id	String	Parameter ID.
req_param_id	String	Request parameter ID.

Table 4-230 CoditionResp

Parameter	Type	Description
req_param_name	String	Input parameter name. This parameter is required if the policy type is param.
sys_param_name	String	Name of a built-in gateway parameter. This parameter is required if the policy type is system. The following parameters are supported: - req_path: request path. For example, /a/b. - req_method: request method. For example, GET. - reqPath: request path, which is discarded. For example, /a/b. - reqMethod: request method, which is discarded. For example, GET.
cookie_param_name	String	COOKIE parameter name. This parameter is required if the policy type is cookie. Minimum: 0 Maximum: 255

Parameter	Type	Description
frontend_authorizer_param_name	String	System parameter: frontend authentication parameter name. This parameter is mandatory when the policy type is frontend_authorizer. The frontend authentication parameter name is prefixed with \$context.authorizer.frontend. For example, if the frontend authentication parameter name is user_name, the name with the prefix will be \$context.authorizer.frontend.user_name.
condition_type	String	Policy condition. • exact: Exact match • enum: Enumeration • pattern: Regular expression This parameter is required when the policy type is param, system, cookie, or frontend_authorizer.
condition_origin	String	Policy type • param: parameter • source: source IP address • system: system parameter - gateway built-in parameter • cookie: COOKIE parameter • frontend_authorizer: system parameter - frontend authentication parameter
condition_value	String	Policy value. Maximum: 1024
mapped_param_name	String	Name of a parameter generated after orchestration. This parameter is mandatory when condition_origin is set to orchestration. The generated parameter name must exist in the orchestration rule bound to the API.
mapped_param_location	String	Location of a parameter generated after orchestration. This parameter is mandatory when condition_origin is set to orchestration. This location must exist in the orchestration rule bound to the API.

Parameter	Type	Description
id	String	ID.
req_param_id	String	Input parameter ID.
req_param_location	String	Input parameter location.

Table 4-231 VpcInfo

Parameter	Type	Description
ecs_id	String	Cloud server ID.
ecs_name	String	Cloud server name.
cascade_flag	Boolean	Indicates whether to use the cascading mode. Currently, this parameter is not supported.
vpc_channel_proxy_host	String	Proxy host.
vpc_channel_id	String	VPC channel ID.
vpc_channel_port	Integer	VPC channel port.

Status code: 400**Table 4-232** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-233** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-234** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-235** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-236** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Modifying an API (authentication mode: app; backend: VPC channel)

```
{
  "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "match_mode" : "NORMAL",
  "name" : "Api_http",
  "auth_type" : "APP",
  "backend_type" : "HTTP",
  "backend_api" : {
    "vpc_channel_status" : 1,
    "vpc_channel_info" : {
      "vpc_channel_id" : "56a7d7358e1b42459c9d730d65b14e59",
      "vpc_channel_proxy_host" : "www.example.com"
    }
  },
  "req_protocol" : "HTTPS",
  "req_method" : "GET",
  "req_uri" : "/test/benchmark",
  "timeout" : 5000,
  "retry_count" : "-1"
},
"cors" : false,
"trace_enabled" : true,
```



```
"sampling_strategy" : "RATE",
"sampling_param" : "10",
"req_protocol" : "HTTPS",
"req_uri" : "/test/http",
"remark" : "Web backend API",
"type" : 1,
"req_method" : "GET",
"result_normal_sample" : "Example success response",
"result_failure_sample" : "Example failure response",
"backend_params" : [ {
  "name" : "X-CONSTANT-HEADER",
  "value" : "demo",
  "location" : "HEADER",
  "origin" : "CONSTANT",
  "remark" : "constant_demo"
}, {
  "name" : "app-id",
  "value" : "$context.appld",
  "location" : "HEADER",
  "origin" : "SYSTEM",
  "remark" : "App ID of the API caller"
} ],
"tags" : [ "webApi" ]
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "5f918d104dc84480a75166ba99efff21",
  "tags" : [ "webApi" ],
  "arrange_necessary" : 2,
  "backend_type" : "HTTP",
  "auth_type" : "APP",
  "auth_opt" : {
    "app_code_auth_type" : "DISABLE"
  },
  "backend_api" : {
    "update_time" : "2020-08-02T16:32:47.077028841Z",
    "vpc_channel_status" : 1,
    "vpc_channel_info" : {
      "vpc_channel_id" : "56a7d7358e1b42459c9d730d65b14e59",
      "vpc_channel_proxy_host" : "www.example.com"
    },
    "url_domain" : "56a7d7358e1b42459c9d730d65b14e59",
    "req_protocol" : "HTTPS",
    "id" : "1ce8fda3586d4371bd83c955df37e102",
    "req_method" : "GET",
    "register_time" : "2020-07-31T12:42:51Z",
    "req_uri" : "/test/benchmark",
    "timeout" : 5000,
    "status" : 1,
    "retry_count" : "-1"
  },
  "cors" : false,
  "trace_enabled" : true,
  "sampling_strategy" : "RATE",
  "sampling_param" : "10",
  "status" : 1,
  "group_name" : "api_group_001",
  "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "group_version" : "V1",
  "match_mode" : "NORMAL",
  "name" : "Api_http",
  "req_protocol" : "HTTPS",
  "req_method" : "GET",
}
```

```
"req_uri" : "/test/http",
"type" : 1,
"version" : "V0.0.1",
"result_normal_sample" : "Example success response",
"result_failure_sample" : "Example failure response",
"register_time" : "2020-07-31T12:42:51Z",
"update_time" : "2020-08-02T16:32:47.046288842Z",
"remark" : "Web backend API",
"backend_params" : [ {
  "name" : "X-CONSTANT-HEADER",
  "value" : "demo",
  "location" : "HEADER",
  "origin" : "CONSTANT",
  "remark" : "constant_demo",
  "id" : "8cb2eba19e7a4423a4e835647a8b8d76"
}, {
  "name" : "app-id",
  "value" : "$context.appld",
  "location" : "HEADER",
  "origin" : "SYSTEM",
  "remark" : "App ID of the API caller",
  "id" : "216ddda836e74d528f364ff589d9dd21"
} ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "API 5f918d104dc84480a75166ba99efff21 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.5.3 Deleting an API

Function

This API is used to delete an API.

This operation will delete all related resources and binding relationships of the API, such as publication records, backend services, and app authorization information.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/apis/{api_id}

Table 4-237 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
api_id	Yes	String	API ID.

Request Parameters

Table 4-238 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 401**Table 4-239** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-240** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-241** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 409

Table 4-242 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500

Table 4-243 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "API 5f918d104dc84480a75166ba99efff21 does not exist"
}
```

Status code: 409

Conflict

```
{
  "error_code" : "APIG.3416",
}
```

```
{
  "error_msg" : "The API cannot be deleted because it has been published"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
401	Unauthorized
403	Forbidden
404	Not Found
409	Conflict
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.5.4 Publishing an API or Taking an API Offline

Function

This API is used to publish an API or take an API offline.

An API can be called only in an environment where the API has been published. APIs that have not been published cannot be called.

You can remove an API from an environment in which it has been published. After this operation, the API can no longer be called in the environment.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/apis/action

Table 4-244 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-245 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-246 Request body parameters

Parameter	Mandatory	Type	Description
action	Yes	String	Operation to perform. • online: publish APIs • offline: take APIs offline
env_id	Yes	String	ID of the environment in which the API will be published.
api_id	Yes	String	ID of the API to be published or taken offline.
remark	No	String	Description about the publishing. It cannot exceed 255 characters.

Response Parameters

Status code: 201

Table 4-247 Response body parameters

Parameter	Type	Description
publish_id	String	Publication record ID.
api_id	String	API ID.
api_name	String	API name.
env_id	String	ID of the environment in which the API has been published.
remark	String	Description about the publication.
publish_time	String	Publication time.
version_id	String	API version currently in use.

Status code: 400**Table 4-248** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-249** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-250** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-251** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-252** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Publishing an API in an environment

```
{
  "action": "online",
  "api_id": "5f918d104dc84480a75166ba99efff21",
  "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID"
}
```

Example Responses

Status code: 201

Created

```
{
  "api_id": "5f918d104dc84480a75166ba99efff21",
  "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "publish_id": "9191cdb430724d4b8586ed7f1b962ca2",
  "publish_time": "2020-08-03T01:36:00.592970615Z",
  "version_id": "ee1a5a38d3d3493abf1dc4ed6cacfa0b"
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2011",
  "error_msg": "Invalid parameter value,parameterName:action. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
}
```

```
{
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3002",
  "error_msg": "API 5f918d104dc84480a75166ba99efff21 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.5.5 Querying API Details

Function

This API is used to query the details of an API.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apis/{api_id}

Table 4-253 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
api_id	Yes	String	API ID.

Request Parameters

Table 4-254 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-255 Response body parameters

Parameter	Type	Description
name	String	API name. It can contain 3 to 255 characters, starting with a letter or digit. Only letters, digits, and these special characters are allowed: -_./:()
type	Integer	API type. 1: public API 2: private API

Parameter	Type	Description
version	String	API version. Maximum: 16
req_protocol	String	API request protocol: • HTTP • HTTPS • BOTH: Both HTTP and HTTPS are supported. • GRPCS Default: HTTPS
req_method	String	API request method. If the request protocol is set to GRPC, the request method is fixed to POST.
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. NOTE The address must comply with the URI specifications.
auth_type	String	API authentication mode. Options: • NONE • APP • IAM • AUTHORIZER: custom authentication. When auth_type is set to AUTHORIZER, the authorizer_id field is mandatory.
auth_opt	AuthOpt object	Security authentication parameter.
cors	Boolean	Indicates whether CORS is supported. • TRUE: supported • FALSE: not supported Default: false
trace_enabled	Boolean	Whether to enable tracing. By default, it is disabled. Default: false

Parameter	Type	Description
sampling_strategy	String	Sampling policy. This parameter is mandatory when tracing is enabled. RATE: sampling by percentage
sampling_param	String	Sampling parameter. When sampling by percentage, the value of this parameter is an integer ranging from 0 to 100. The default value is 100, which indicates all requests are sampled. It is recommended that align the value with the backend sampling percentage. Default: 100 Minimum: 1 Maximum: 64
match_mode	String	API matching mode: - SWA: Prefix match - NORMAL: Exact match Default value: NORMAL
backend_type	String	Backend type. Options: - HTTP: web backend - FUNCTION: FunctionGraph backend. When backend_type is set to FUNCTION, the func_info field is mandatory. - MOCK: mock backend. When backend_type is set to MOCK, the mock_info field is mandatory. - GRPC: gRPC backend.
remark	String	API description. It cannot exceed 255 characters.
group_id	String	ID of the API group to which the API belongs.
body_remark	String	API request body, which can be an example request body, media type, or parameters. Ensure that the request body does not exceed 20,480 characters.

Parameter	Type	Description
result_normal_sample	String	Example response for a successful request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.
result_failure_sample	String	Example response for a failed request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.
authorizer_id	String	ID of the frontend custom authorizer
tags	Array of strings	Tag. Use letters, digits, and special characters (-*#%.:_) and start with a letter. By default, 10 tags are supported. To increase the quota, contact technical support to modify the API_TAG_NUM_LIMIT configuration. Minimum: 1 Maximum: 128
response_id	String	Group response ID.
roma_app_id	String	Integration application ID. Currently, this parameter is not supported.
domain_name	String	Custom domain name bound to the API. Currently, this parameter is not supported.
tag	String	Tag. This field will be deprecated. You can use the tags field instead.
content_type	String	Request content type: application/json application/xml multipart/form-data text/plain

Parameter	Type	Description
is_send_fg_body_base64	Boolean	Specifies whether to perform Base64 encoding on the body for interaction with FunctionGraph. The body does not need to be encoded using Base64 only when content_type is set to application/json. Application scenario: - Custom authentication - Bound circuit breaker plug-in with FunctionGraph backend downgrade policy - APIs with FunctionGraph backend Default: true
id	String	API ID.
status	Integer	App status. 1: valid
arrange_necessary	Integer	Indicates whether to enable orchestration.
register_time	String	Time when the API is registered.
update_time	String	Time when the API was last modified.
group_name	String	Name of the API group to which the API belongs.
group_version	String	Version of the API group to which the API belongs. The default value is V1. Other versions are not supported. Default: V1
run_env_id	String	ID of the environment in which the API has been published. Separate multiple environment IDs with vertical bars ().
run_env_name	String	Name of the environment in which the API has been published. Separate multiple environment names with vertical bars ().
publish_id	String	Publication record ID. Separate multiple publication record IDs with vertical bars ().

Parameter	Type	Description
publish_time	String	Publication time. Separate the time of multiple publication records with vertical bars ().
roma_app_name	String	Name of the integration application to which the API belongs. Currently, this parameter is not supported.
ld_api_id	String	ID of the corresponding custom backend API. Currently, this parameter is not supported.
backend_api	BackendApi object	Web backend details.
api_group_info	ApiGroupCommonInfo object	API group information.
func_info	ApiFunc object	FunctionGraph backend details.
mock_info	ApiMock object	Mock backend details.
req_params	Array of ReqParam objects	Request parameters.
backend_params	Array of BackendParam objects	Backend parameters.
policy_functions	Array of ApiPolicyFunctionResp objects	FunctionGraph backend policies.
policy_mock	Array of ApiPolicyMockResp objects	Mock backend policies.
policy_https	Array of ApiPolicyHttpResp objects	Web backend policies.

Table 4-256 AuthOpt

Parameter	Type	Description
app_code_auth_type	String	Indicates whether AppCode authentication is enabled. This parameter is valid only if auth_type is set to App. The default value is DISABLE. - DISABLE: AppCode authentication is disabled. - HEADER: AppCode authentication is enabled and the AppCode is located in the header. Default: DISABLE

Table 4-257 BackendApi

Parameter	Type	Description
authorizer_id	String	Backend custom authorizer ID.
url_domain	String	Address of the backend service. This parameter is required when no VPC channel is used. It consists of a domain name or IP address and a port number. Maximum length: 255 characters. It must be in the format "Host name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
req_protocol	String	Request protocol. You can select GRPC or GRPCS for the GRPC backend.
remark	String	Description. It cannot exceed 255 characters.
req_method	String	Request method. For the GRPC backend, the request method is fixed to POST.
version	String	Web backend version, which can contain a maximum of 16 characters.

Parameter	Type	Description
req_uri	String	Request address, which can contain request parameters enclosed with braces {}. For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications. For the GRPC backend, the request address is fixed to /.
timeout	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms. Minimum: 1
enable_client_ssl	Boolean	Indicates whether to enable two-way authentication.
retry_count	String	Number of retry attempts to request the backend service. The default value is -1. The value ranges from -1 to 10. -1 indicates that idempotent APIs will retry once and non-idempotent APIs will not retry. POST and PATCH are non-idempotent. GET, HEAD, PUT, OPTIONS, and DELETE are idempotent. Default: -1
enable_sm_channel	Boolean	Indicates whether to enable SM cryptographic algorithms. This feature is only available if the gateway supports the SM cryptographic algorithms.
id	String	ID.

Parameter	Type	Description
status	Integer	Backend service status. 1: valid
register_time	String	Registration time.
update_time	String	Update time.
vpc_channel_info	VpcInfo object	VPC channel details. This parameter is required if vpc_channel_status is set to 1.
vpc_channel_status	Integer	Indicates whether to use a VPC channel. 1: A VPC channel is used. 2: No VPC channel is used.

Table 4-258 ApiGroupCommonInfo

Parameter	Type	Description
id	String	ID.
name	String	API group name.
status	Integer	Status. 1: valid
sl_domain	String	Subdomain name that APIG automatically allocates to the API group.
register_time	String	Creation time.
update_time	String	Last modification time.
on_sell_status	Integer	Indicates whether the API group has been listed on KooGallery. 1: listed 2: not listed 3: under review Not supported currently.
url_domains	Array of UrlDomain objects	Independent domain names bound to the API group.
sl_domain_access_enabled	Boolean	Whether the debugging domain name is accessible. Options: true and false. Default: true

Table 4-259 UrlDomain

Parameter	Type	Description
id	String	Domain ID.
domain	String	Domain name.
cname_status	Integer	CNAME resolution status of the domain name. • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
min_ssl_version	String	Minimum SSL version. TLS 1.1 and TLS 1.2 are supported. Default: TLSv1.1
verified_client_certificate_enabled	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false
is_has_trusted_root_ca	Boolean	Whether a trusted root certificate (CA) exists. The value is true if trusted_root_ca exists in the bound certificate. Default: false

Parameter	Type	Description
ingress_http_port	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ingress_https_port	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ssl_infos	Array of SslInfo objects	SSL certificate list.

Table 4-260 SslInfo

Parameter	Type	Description
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2
type	String	Certificate scope: • instance • global Default: global

Table 4-261 ApiFunc

Parameter	Type	Description
function_urn	String	Function URN.
remark	String	Description. It cannot exceed 255 characters.
invocation_type	String	Invocation mode. • async: asynchronous • sync: synchronous
network_type	String	Function network architecture. • V1: non-VPC • V2: VPC
version	String	Function version. If both a function alias URN and version are passed, only the alias URN will be used. Maximum: 64
alias_urn	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.

Parameter	Type	Description
timeout	Integer	Timeout allowed for APIG to request the backend service. If the function network architecture is set to V1, the maximum timeout is 60,000. If the network architecture is set to V2, the maximum timeout is 600,000 and can be modified by using the gateway parameter backend_timeout. Unit: ms. Minimum: 1
authorizer_id	String	Backend custom authorizer ID.
req_protocol	String	Backend request protocol of a function. The value can be HTTPS (default) or GRPCS (available when the frontend request protocol is GRPCS). Default: HTTPS
id	String	ID.
register_time	String	Registration time.
status	Integer	Backend service status. • 1: valid
update_time	String	Update time.

Table 4-262 ApiMock

Parameter	Type	Description
remark	String	Description. It cannot exceed 255 characters.
result_content	String	Response.
version	String	Function version. It cannot exceed 64 characters.
authorizer_id	String	Backend custom authorizer ID.
id	String	ID.
register_time	String	Registration time.
status	Integer	Backend service status. • 1: valid
update_time	String	Update time.

Table 4-263 ReqParam

Parameter	Type	Description
name	String	Parameter name. The parameter name can contain 1 to 32 characters and must start with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
type	String	Parameter type.
location	String	Parameter location.
default_value	String	Default value.
sample_value	String	Example value.
required	Integer	Indicates whether the parameter is required. 1: yes 2: no The value of this parameter is 1 if Location is set to PATH, and 2 if Location is set to another value.
valid_enable	Integer	Indicates whether validity check is enabled. 1: enabled 2: disabled Default: 2
remark	String	Description. It cannot exceed 255 characters.
enumerations	String	Enumerated value.
min_num	Integer	Minimum value. This parameter is valid when type is set to NUMBER.
max_num	Integer	Maximum value. This parameter is valid when type is set to NUMBER.
min_size	Integer	Minimum length. This parameter is valid when type is set to STRING.
max_size	Integer	Maximum length. This parameter is valid when type is set to STRING.

Parameter	Type	Description
regular	String	Regular expression validation rule. Currently, this parameter is not supported.
json_schema	String	JSON validation rule. Currently, this parameter is not supported.
pass_through	Integer	Indicates whether to transparently transfer the parameter. 1: yes 2: no
orchestrations	Array of strings	Request parameter orchestration rules are prioritized in the same sequence as the list. The none_value rule in a rule list has the highest priority. A maximum of one none_value rule can be bound. The default rule in a rule list has the lowest priority. A maximum of one default rule can be bound. The preprocessing orchestration rule cannot be used as the last orchestration rule except the default rule. Only one parameter of each API can be bound with unique orchestration rules. The number of orchestration rules that can be bound is limited by quota. For details, see "Notes and Constraints" in APIG Service Overview.
id	String	Parameter ID.

Table 4-264 ApiPolicyFunctionResp

Parameter	Type	Description
function_urn	String	Function URN.
invocation_type	String	Invocation mode. • async: asynchronous • sync: synchronous

Parameter	Type	Description
network_type	String	Function network architecture. • V1: non-VPC • V2: VPC
version	String	Function version. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored. Maximum: 64
alias_urn	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
timeout	Integer	Timeout allowed for APIG to request the backend service. If the function network architecture is set to V1, the maximum timeout is 60,000. If the network architecture is set to V2, the maximum timeout is 600,000 and can be modified by using the gateway parameter backend_timeout. Unit: ms. Minimum: 1
req_protocol	String	Backend request protocol of a function. The value can be HTTPS (default) or GRPCS (available when the frontend request protocol is GRPCS). Default: HTTPS
id	String	ID.
effect_mode	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	String	Backend name, which must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64

Parameter	Type	Description
backend_params	Array of BackendParam objects	Backend parameters.
conditions	Array of CoditionResp objects	Policy conditions.
authorizer_id	String	Backend custom authorizer ID.

Table 4-265 ApiPolicyMockResp

Parameter	Type	Description
id	String	ID.
effect_mode	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	String	Backend name, which must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_params	Array of BackendParam objects	Backend parameters.
conditions	Array of CoditionResp objects	Policy conditions.
authorizer_id	String	Backend custom authorizer ID.
result_content	String	Response.

Table 4-266 ApiPolicyHttpResp

Parameter	Type	Description
id	String	ID.
effect_mode	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.

Parameter	Type	Description
name	String	Backend name, which must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_params	Array of BackendParam objects	Backend parameters.
conditions	Array of CoditionResp objects	Policy conditions.
authorizer_id	String	Backend custom authorizer ID.
url_domain	String	Endpoint of the policy backend. An endpoint consists of a domain name or IP address and a port number, with not more than 255 characters. It must be in the format "Domain name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
req_protocol	String	Request protocol. Options include HTTP, HTTPS, GRPC, or GRPCS. You can select GRPC or GRPCS for the GRPC backend.
req_method	String	Request method. Options include GET, POST, PUT, DELETE, HEAD, PATCH, OPTIONS, and ANY. This is fixed to POST for the GRPC backend.

Parameter	Type	Description
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications. For the GRPC backend, the request address is fixed to /.
timeout	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms. Minimum: 1
retry_count	String	Number of retry attempts to request the backend service. The default value is -1. The value ranges from -1 to 10. -1 indicates that idempotent APIs will retry once and non-idempotent APIs will not retry. POST and PATCH are non-idempotent. GET, HEAD, PUT, OPTIONS, and DELETE are idempotent. Default: -1
enable_sm_channel	Boolean	Indicates whether to enable SM cryptographic algorithms. This feature is only available if the gateway supports the SM cryptographic algorithms.
vpc_channel_info	VpcInfo object	VPC channel details. This parameter is required if vpc_channel_status is set to 1.

Parameter	Type	Description
vpc_channel_status	Integer	Indicates whether to use a VPC channel. • 1: A VPC channel is used. • 2: No VPC channel is used.

Table 4-267 BackendParam

Parameter	Type	Description
origin	String	Parameter type. • REQUEST: backend parameter • CONSTANT: constant parameter • SYSTEM: system parameter
name	String	Parameter name. The parameter name must start with a letter and can only contain letters, digits, hyphens (-), underscores (_), and periods (.). Minimum: 1 Maximum: 32
remark	String	Description, which can contain a maximum of 255 characters.
location	String	Parameter location. The value can be PATH, QUERY, or HEADER.

Parameter	Type	Description
value	String	Parameter value, which can contain a maximum of 255 characters. If the origin type is REQUEST, the value of this parameter is the parameter name in req_params. If the origin type is CONSTANT, the value is a constant. If the origin type is SYSTEM, the value is a system parameter name. System parameters include gateway parameters, frontend authentication parameters, and backend authentication parameters. You can set the frontend or backend authentication parameters after enabling custom frontend or backend authentication. The gateway parameters are as follows: • \$context.sourceIp: source IP address of the API caller. • \$context.stage: deployment environment in which the API is called. • \$context.apid: API ID. • \$context.appId: ID of the app used by the API caller. • \$context.requestId: request ID generated when the API is called. • \$context.serverAddr: address of the gateway server. • \$context.serverName: name of the gateway server. • \$context.handleTime: time when the API request is processed. • \$context.providerAppId: ID of the app used by the API owner. This parameter is currently not supported. Frontend authentication parameter: prefixed with "\$context.authorizer.frontend.". For example, to return "aaa" upon successful custom authentication, set this parameter to "\$context.authorizer.frontend.aaa".

Parameter	Type	Description
		Backend authentication parameter: prefixed with "\$context.authorizer.backend.". For example, to return "aaa" upon successful custom authentication, set this parameter to "\$context.authorizer.backend.aaa".
id	String	Parameter ID.
req_param_id	String	Request parameter ID.

Table 4-268 CoditionResp

Parameter	Type	Description
req_param_name	String	Input parameter name. This parameter is required if the policy type is param.
sys_param_name	String	Name of a built-in gateway parameter. This parameter is required if the policy type is system. The following parameters are supported: - req_path: request path. For example, /a/b. - req_method: request method. For example, GET. - reqPath: request path, which is discarded. For example, /a/b. - reqMethod: request method, which is discarded. For example, GET.
cookie_param_name	String	COOKIE parameter name. This parameter is required if the policy type is cookie. Minimum: 0 Maximum: 255

Parameter	Type	Description
frontend_authorizer_param_name	String	System parameter: frontend authentication parameter name. This parameter is mandatory when the policy type is frontend_authorizer. The frontend authentication parameter name is prefixed with \$context.authorizer.frontend. For example, if the frontend authentication parameter name is user_name, the name with the prefix will be \$context.authorizer.frontend.user_name.
condition_type	String	Policy condition. • exact: Exact match • enum: Enumeration • pattern: Regular expression This parameter is required when the policy type is param, system, cookie, or frontend_authorizer.
condition_origin	String	Policy type • param: parameter • source: source IP address • system: system parameter - gateway built-in parameter • cookie: COOKIE parameter • frontend_authorizer: system parameter - frontend authentication parameter
condition_value	String	Policy value. Maximum: 1024
mapped_param_name	String	Name of a parameter generated after orchestration. This parameter is mandatory when condition_origin is set to orchestration. The generated parameter name must exist in the orchestration rule bound to the API.
mapped_param_location	String	Location of a parameter generated after orchestration. This parameter is mandatory when condition_origin is set to orchestration. This location must exist in the orchestration rule bound to the API.

Parameter	Type	Description
id	String	ID.
req_param_id	String	Input parameter ID.
req_param_location	String	Input parameter location.

Table 4-269 VpcInfo

Parameter	Type	Description
ecs_id	String	Cloud server ID.
ecs_name	String	Cloud server name.
cascade_flag	Boolean	Indicates whether to use the cascading mode. Currently, this parameter is not supported.
vpc_channel_proxy_host	String	Proxy host.
vpc_channel_id	String	VPC channel ID.
vpc_channel_port	Integer	VPC channel port.

Status code: 401**Table 4-270** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-271** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-272 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-273 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "id" : "5f918d104dc84480a75166ba99efff21",
  "tags" : [ "webApi" ],
  "arrange_necessary" : 2,
  "backend_type" : "HTTP",
  "auth_type" : "AUTHORIZER",
  "auth_opt" : {
    "app_code_auth_type" : "DISABLE"
  },
  "authorizer_id" : "8d0443832a194eaa84244e0c1c1912ac",
  "backend_api" : {
    "update_time" : "2020-08-02T16:32:47.077029Z",
    "vpc_channel_status" : 1,
    "vpc_channel_info" : {
      "vpc_channel_id" : "56a7d7358e1b42459c9d730d65b14e59",
      "vpc_channel_proxy_host" : "www.example.com"
    },
  },
  "url_domain" : "56a7d7358e1b42459c9d730d65b14e59",
  "req_protocol" : "HTTPS",
  "id" : "1ce8fda3586d4371bd83c955df37e102",
  "req_method" : "GET",
  "register_time" : "2020-07-31T12:42:51Z",
  "req_uri" : "/test/benchmark",
  "timeout" : 5000,
  "status" : 1,
  "retry_count" : "-1"
},
"cors" : false,
```

```
"trace_enabled" : true,
"sampling_strategy" : "RATE",
"sampling_param" : "10",
"status" : 1,
"group_name" : "api_group_001",
"group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
"group_version" : "V1",
"match_mode" : "NORMAL",
"name" : "Api_http",
"req_protocol" : "HTTPS",
"req_method" : "GET",
"req_uri" : "/test/http",
"type" : 1,
"version" : "V0.0.1",
"result_normal_sample" : "Example success response",
"result_failure_sample" : "Example failure response",
"register_time" : "2020-07-31T12:42:51Z",
"update_time" : "2020-08-02T16:32:47.046289Z",
"remark" : "Web backend API",
"backend_params" : [ {
  "name" : "X-CONSTANT-HEADER",
  "value" : "demo",
  "location" : "HEADER",
  "origin" : "CONSTANT",
  "remark" : "constant_demo",
  "id" : "8cb2eba19e7a4423a4e835647a8b8d76"
}, {
  "name" : "app-id",
  "value" : "$context.appId",
  "location" : "HEADER",
  "origin" : "SYSTEM",
  "remark" : "App ID of the API caller",
  "id" : "216ddda836e74d528f364ff589d9dd21"
} ]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "API 5f918d104dc84480a75166ba99efff21 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
}
```

```
"error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.5.6 Querying APIs

Function

This API is used to query APIs to return their details and publication information. Backend and request parameter information of the APIs will not be returned.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apis

Table 4-274 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-275 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
id	No	String	API ID.
name	No	String	API name.
group_id	No	String	API group ID.
req_protocol	No	String	Request protocol.
req_method	No	String	Request method.
req_uri	No	String	Request path.
auth_type	No	String	Security authentication mode.
env_id	No	String	ID of the environment in which the API has been published.
type	No	Integer	API type.
precise_search	No	String	Parameter name (name or req_uri) for exact matching.
vpc_channel_name	No	String	Load balance channel name.

Parameter	Mandatory	Type	Description
return_data_mode	No	String	Additional information to be included in the returned API details. Separate multiple parameters with commas (.). "brief" does not take effect when used with any "include" parameters. Currently, only brief, include_group, and include_group_backend are supported. brief: default, indicating that no additional information will be included. include_group: The return result will include api_group_info. include_group_backend: The return result will include backend_api. Default: brief
tags	No	String	API tag. Multiple API tags can be specified. The relationship between multiple parameter values is OR. If this parameter is not specified, no filtering tag is specified. If this parameter is set to #no_tags#, APIs without tags are filtered. Minimum: 0 Maximum: 128

Request Parameters

Table 4-276 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-277 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
apis	Array of ApiInfoPerPage objects	API list.

Table 4-278 ApiInfoPerPage

Parameter	Type	Description
name	String	API name. It can contain 3 to 255 characters, starting with a letter or digit. Only letters, digits, and these special characters are allowed: -_./:()
type	Integer	API type. 1: public API 2: private API
version	String	API version. Maximum: 16
req_protocol	String	API request protocol: - HTTP - HTTPS - BOTH: Both HTTP and HTTPS are supported. - GRPCS Default: HTTPS
req_method	String	API request method. If the request protocol is set to GRPCS, the request method is fixed to POST.

Parameter	Type	Description
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. NOTE The address must comply with the URI specifications.
auth_type	String	API authentication mode. Options: • NONE • APP • IAM • AUTHORIZER: custom authentication. When auth_type is set to AUTHORIZER, the authorizer_id field is mandatory.
auth_opt	AuthOpt object	Security authentication parameter.
cors	Boolean	Indicates whether CORS is supported. • TRUE: supported • FALSE: not supported Default: false
trace_enabled	Boolean	Whether to enable tracing. By default, it is disabled. Default: false
sampling_strategy	String	Sampling policy. This parameter is mandatory when tracing is enabled. • RATE: sampling by percentage

Parameter	Type	Description
sampling_param	String	Sampling parameter. When sampling by percentage, the value of this parameter is an integer ranging from 0 to 100. The default value is 100, which indicates all requests are sampled. It is recommended that align the value with the backend sampling percentage. Default: 100 Minimum: 1 Maximum: 64
match_mode	String	API matching mode: - SWA: Prefix match - NORMAL: Exact match Default value: NORMAL
backend_type	String	Backend type. Options: - HTTP: web backend - FUNCTION: FunctionGraph backend. When backend_type is set to FUNCTION, the func_info field is mandatory. - MOCK: mock backend. When backend_type is set to MOCK, the mock_info field is mandatory. - GRPC: gRPC backend.
remark	String	API description. It cannot exceed 255 characters.
group_id	String	ID of the API group to which the API belongs.
body_remark	String	API request body, which can be an example request body, media type, or parameters. Ensure that the request body does not exceed 20,480 characters.
result_normal_sample	String	Example response for a successful request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.

Parameter	Type	Description
result_failure_sample	String	Example response for a failed request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.
authorizer_id	String	ID of the frontend custom authorizer
tags	Array of strings	Tag. Use letters, digits, and special characters (-*#%.:_) and start with a letter. By default, 10 tags are supported. To increase the quota, contact technical support to modify the API_TAG_NUM_LIMIT configuration. Minimum: 1 Maximum: 128
response_id	String	Group response ID.
roma_app_id	String	Integration application ID. Currently, this parameter is not supported.
domain_name	String	Custom domain name bound to the API. Currently, this parameter is not supported.
tag	String	Tag. This field will be deprecated. You can use the tags field instead.
content_type	String	Request content type: application/json application/xml multipart/form-data text/plain

Parameter	Type	Description
is_send_fg_body_base64	Boolean	Specifies whether to perform Base64 encoding on the body for interaction with FunctionGraph. The body does not need to be encoded using Base64 only when content_type is set to application/json. Application scenario: • Custom authentication • Bound circuit breaker plug-in with FunctionGraph backend downgrade policy • APIs with FunctionGraph backend Default: true
id	String	API ID.
status	Integer	App status. • 1: valid
arrange_necessary	Integer	Indicates whether to enable orchestration.
register_time	String	Time when the API is registered.
update_time	String	Time when the API was last modified.
group_name	String	Name of the API group to which the API belongs.
group_version	String	Version of the API group to which the API belongs. The default value is V1. Other versions are not supported. Default: V1
run_env_id	String	ID of the environment in which the API has been published. Separate multiple environment IDs with vertical bars ().
run_env_name	String	Name of the environment in which the API has been published. Separate multiple environment names with vertical bars ().
publish_id	String	Publication record ID. Separate multiple publication record IDs with vertical bars ().

Parameter	Type	Description
publish_time	String	Publication time. Separate the time of multiple publication records with vertical bars ().
roma_app_name	String	Name of the integration application to which the API belongs. Currently, this parameter is not supported.
ld_api_id	String	ID of the corresponding custom backend API. Currently, this parameter is not supported.
backend_api	BackendApi object	Backend information.
api_group_info	ApiGroupCommonInfo object	API group information.
req_params	Array of ReqParam objects	Request parameters.

Table 4-279 AuthOpt

Parameter	Type	Description
app_code_auth_type	String	Indicates whether AppCode authentication is enabled. This parameter is valid only if auth_type is set to App. The default value is DISABLE. - DISABLE: AppCode authentication is disabled. - HEADER: AppCode authentication is enabled and the AppCode is located in the header. Default: DISABLE

Table 4-280 BackendApi

Parameter	Type	Description
authorizer_id	String	Backend custom authorizer ID.

Parameter	Type	Description
url_domain	String	Address of the backend service. This parameter is required when no VPC channel is used. It consists of a domain name or IP address and a port number. Maximum length: 255 characters. It must be in the format "Host name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
req_protocol	String	Request protocol. You can select GRPC or GRPCS for the GRPC backend.
remark	String	Description. It cannot exceed 255 characters.
req_method	String	Request method. For the GRPC backend, the request method is fixed to POST.
version	String	Web backend version, which can contain a maximum of 16 characters.
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications. For the GRPC backend, the request address is fixed to /.

Parameter	Type	Description
timeout	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms. Minimum: 1
enable_client_ssl	Boolean	Indicates whether to enable two-way authentication.
retry_count	String	Number of retry attempts to request the backend service. The default value is -1. The value ranges from -1 to 10. -1 indicates that idempotent APIs will retry once and non-idempotent APIs will not retry. POST and PATCH are non-idempotent. GET, HEAD, PUT, OPTIONS, and DELETE are idempotent. Default: -1
enable_sm_channel	Boolean	Indicates whether to enable SM cryptographic algorithms. This feature is only available if the gateway supports the SM cryptographic algorithms.
id	String	ID.
status	Integer	Backend service status. 1: valid
register_time	String	Registration time.
update_time	String	Update time.
vpc_channel_info	VpcInfo object	VPC channel details. This parameter is required if vpc_channel_status is set to 1.
vpc_channel_status	Integer	Indicates whether to use a VPC channel. 1: A VPC channel is used. 2: No VPC channel is used.

Table 4-281 VpcInfo

Parameter	Type	Description
ecs_id	String	Cloud server ID.
ecs_name	String	Cloud server name.
cascade_flag	Boolean	Indicates whether to use the cascading mode. Currently, this parameter is not supported.
vpc_channel_proxy_host	String	Proxy host.
vpc_channel_id	String	VPC channel ID.
vpc_channel_port	Integer	VPC channel port.

Table 4-282 ApiGroupCommonInfo

Parameter	Type	Description
id	String	ID.
name	String	API group name.
status	Integer	Status. 1: valid
sl_domain	String	Subdomain name that APIG automatically allocates to the API group.
register_time	String	Creation time.
update_time	String	Last modification time.
on_sell_status	Integer	Indicates whether the API group has been listed on KooGallery. 1: listed 2: not listed 3: under review Not supported currently.
url_domains	Array of UrlDomain objects	Independent domain names bound to the API group.
sl_domain_access_enabled	Boolean	Whether the debugging domain name is accessible. Options: true and false. Default: true

Table 4-283 UrlDomain

Parameter	Type	Description
id	String	Domain ID.
domain	String	Domain name.
cname_status	Integer	CNAME resolution status of the domain name. • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
min_ssl_version	String	Minimum SSL version. TLS 1.1 and TLS 1.2 are supported. Default: TLSv1.1
verified_client_certificate_enabled	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false
is_has_trusted_root_ca	Boolean	Whether a trusted root certificate (CA) exists. The value is true if trusted_root_ca exists in the bound certificate. Default: false

Parameter	Type	Description
ingress_http_port	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ingress_https_port	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ssl_infos	Array of SslInfo objects	SSL certificate list.

Table 4-284 SslInfo

Parameter	Type	Description
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2
type	String	Certificate scope: • instance • global Default: global

Table 4-285 ReqParam

Parameter	Type	Description
name	String	Parameter name. The parameter name can contain 1 to 32 characters and must start with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
type	String	Parameter type.
location	String	Parameter location.
default_value	String	Default value.
sample_value	String	Example value.
required	Integer	Indicates whether the parameter is required. 1: yes 2: no The value of this parameter is 1 if Location is set to PATH, and 2 if Location is set to another value.
valid_enable	Integer	Indicates whether validity check is enabled. • 1: enabled • 2: disabled Default: 2

Parameter	Type	Description
remark	String	Description. It cannot exceed 255 characters.
enumerations	String	Enumerated value.
min_num	Integer	Minimum value. This parameter is valid when type is set to NUMBER.
max_num	Integer	Maximum value. This parameter is valid when type is set to NUMBER.
min_size	Integer	Minimum length. This parameter is valid when type is set to STRING.
max_size	Integer	Maximum length. This parameter is valid when type is set to STRING.
regular	String	Regular expression validation rule. Currently, this parameter is not supported.
json_schema	String	JSON validation rule. Currently, this parameter is not supported.
pass_through	Integer	Indicates whether to transparently transfer the parameter. 1: yes 2: no

Parameter	Type	Description
orchestrations	Array of strings	Request parameter orchestration rules are prioritized in the same sequence as the list. The none_value rule in a rule list has the highest priority. A maximum of one none_value rule can be bound. The default rule in a rule list has the lowest priority. A maximum of one default rule can be bound. The preprocessing orchestration rule cannot be used as the last orchestration rule except the default rule. Only one parameter of each API can be bound with unique orchestration rules. The number of orchestration rules that can be bound is limited by quota. For details, see "Notes and Constraints" in APIG Service Overview.
id	String	Parameter ID.

Status code: 400**Table 4-286** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-287** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-288 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-289 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 3,
  "size" : 3,
  "apis" : [ {
    "arrange_necessary" : 2,
    "id" : "5f918d104dc84480a75166ba99efff21",
    "tags" : [ "webApi" ],
    "backend_type" : "HTTP",
    "auth_type" : "AUTHORIZER",
    "auth_opt" : {
      "app_code_auth_type" : "DISABLE"
    },
    "authorizer_id" : "8d0443832a194eaa84244e0c1c1912ac",
    "cors" : false,
    "trace_enabled" : true,
    "sampling_strategy" : "RATE",
    "sampling_param" : "10",
    "status" : 1,
    "group_name" : "api_group_001",
    "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
    "group_version" : "V1",
    "match_mode" : "NORMAL",
    "name" : "Api_http",
    "req_protocol" : "HTTPS",
    "req_method" : "GET",
    "req_uri" : "/test/http",
    "type" : 1,
    "version" : "V0.0.1",
    "register_time" : "2020-07-31T12:42:51Z",
    "update_time" : "2020-08-02T16:32:47.046289Z",
    "remark" : "Web backend API"
  } ]
}
```

```
{
  {
    "id": "3a955b791bd24b1c9cd94c745f8d1aad",
    "group_id": "c77f5e81d9cb4424bf704ef2b0ac7600",
    "group_name": "api_group_001",
    "group_version": "V1",
    "match_mode": "SWA",
    "name": "Api_mock",
    "auth_type": "IAM",
    "auth_opt": {
      "auth_code_auth_type": "DISABLE"
    },
    "backend_type": "MOCK",
    "cors": false,
    "req_protocol": "HTTPS",
    "req_uri": "/test/mock",
    "remark": "Mock backend API",
    "type": 1,
    "version": "V0.0.1",
    "req_method": "GET",
    "result_normal_sample": "Example success response",
    "result_failure_sample": "Example failure response",
    "tags": [ "mockApi" ],
    "register_time": "2020-08-02T15:56:52Z",
    "update_time": "2020-08-02T15:56:52Z",
    "status": 1
  }, {
    "id": "abd9c4b2ff974888b0ba79be7e6b2763",
    "arrange_necessary": 2,
    "group_id": "c77f5e81d9cb4424bf704ef2b0ac7600",
    "group_name": "api_group_001",
    "group_version": "V1",
    "match_mode": "NORMAL",
    "name": "Api_function",
    "auth_type": "APP",
    "auth_opt": {
      "auth_code_auth_type": "DISABLE"
    },
    "backend_type": "FUNCTION",
    "cors": false,
    "req_protocol": "HTTPS",
    "req_uri": "/test/function",
    "remark": "FunctionGraph backend API",
    "type": 1,
    "version": "V0.0.1",
    "status": 1,
    "req_method": "GET",
    "tags": [ "functionApi" ],
    "register_time": "2020-08-02T15:36:19Z",
    "update_time": "2020-08-02T15:47:53.499266Z"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2012",
  "error_msg": "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error CodesSee [Error Codes](#).**4.5.7 Verifying the API Definition****Function**

This API is used to verify the API definition, that is, whether the API path or name already exists.

Calling MethodFor details, see [Calling APIs](#).**URI**

POST /v2/{project_id}/apigw/instances/{instance_id}/apis/check

Table 4-290 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-291 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-292 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	API name. This parameter is mandatory when type is set to name.
req_method	No	String	Request method. This parameter is mandatory when type is set to path.
req_uri	No	String	Access address of the API. This parameter is mandatory when type is set to path.
match_mode	No	String	API matching mode: • SWA: Prefix match • NORMAL: Exact match This parameter is mandatory when type is set to path.

Parameter	Mandatory	Type	Description
group_id	No	String	Group ID. This parameter is mandatory for checking for duplicate API definitions in the group.
roma_app_id	No	String	Integration application ID. This is not supported currently.
api_id	No	String	ID of the API to be compared.
type	Yes	String	Verification type: • path: path type • name: name type

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-293 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401

Table 4-294 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403

Table 4-295 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-296** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-297** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

```
{
  "type" : "name",
  "name" : "api_demo"
}
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.3202",
  "error_msg" : "The API name already exists, api_name:api_demo"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:f0fa1789-3b76-433b-a787-9892951c620ec"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.5.8 Debugging an API

Function

This API is used to debug an API in a specified environment. The API caller must have the permissions required for accessing this API.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/apis/debug/{api_id}

Table 4-298 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
api_id	Yes	String	API ID.

Request Parameters

Table 4-299 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-300 Request body parameters

Parameter	Mandatory	Type	Description
body	No	String	Message body, with a maximum of 2,097,152 bytes.

Parameter	Mandatory	Type	Description
header	No	Map<String,Array<String>>	Header parameters, with each value being a character string array. Each parameter name must meet the following requirements: • Contains letters, digits, periods (.), or hyphens (-). • Starts with a letter, with a maximum of 32 bytes. • Case-insensitive and cannot start with X-Apig- or X-Sdk-. • Case-insensitive and cannot be X-Stage. • Case-insensitive and cannot be X-Auth-Token or Authorization when mode is set to MARKET or CONSUMER. NOTE Each header name is normalized before use. For example, x-MY-hEaDer is normalized as X-My-Header.
method	Yes	String	API request method.
mode	Yes	String	Debugging mode: • DEVELOPER: Debug the definitions of an API that has not been published. • CONSUMER: Debug the definitions of an API that has been published in a specified environment. NOTE In DEVELOPER mode, the API caller must be the API provider. In CONSUMER mode, the API caller must be the API provider or has been authorized to access the API in a specific environment.

Parameter	Mandatory	Type	Description
path	Yes	String	Request path of the API, starting with a slash (/) and containing up to 1024 characters. NOTE The request path must meet the requirements so that it can be correctly decoded after percent-encoding.
query	No	Map<String,Array<String>>	Query strings, with each value being a character string array. Each parameter name must meet the following requirements: • Contains letters, digits, periods (.), hyphens (-), or underscores (_). • Starts with a letter, with a maximum of 32 bytes. • Case-insensitive and cannot start with X-Apig- or X-Sdk-. • Case-insensitive and cannot be X-Stage.
scheme	Yes	String	Request protocol. • HTTP • HTTPS
app_key	No	String	AppKey used in the debugging request.
app_secret	No	String	AppSecret used in the debugging request.

Parameter	Mandatory	Type	Description
domain	No	String	Access domain name of the API. For gateways with custom inbound ports, the port information must be contained and separated by colons (:), for example, test.com:8080. If no value is specified, one of the following default values will be used based on the mode: • DEVELOPER: The subdomain name of the API group will be used. • MARKET: This parameter is not used currently. • CONSUMER: The subdomain name of the API group will be used.
stage	No	String	Running environment specified by the debugging request. This parameter is valid only when mode is set to CONSUMER. If this parameter is not specified, the following default value is used: • CONSUMER RELEASE

Response Parameters

Status code: 200

Table 4-301 Response body parameters

Parameter	Type	Description
request	String	Body of the debugging request.
response	String	Body of the debugging response, with a maximum of 2,097,152 bytes. Any content beyond this threshold will be truncated. NOTE Any content beyond the length limit will be truncated, and text [TRUNCATED] will be added to the response body.

Parameter	Type	Description
latency	Integer	Debugging duration in milliseconds.
log	String	Debugging logs.

Status code: 400**Table 4-302** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-303** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-304** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-305** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-306** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Debugging an API

```
{
  "mode" : "DEVELOPER",
  "scheme" : "HTTPS",
  "method" : "GET",
  "path" : "/test/mock"
}
```

Example Responses

Status code: 200

OK

```
{
  "request" : "GET /test/mock HTTP/1.1\nHost: c77f5e81d9cb4424bf704ef2b0ac7600.apic.****.com\nUser-Agent: APIGatewayDebugClient/1.0\nX-Apig-Mode: debug\n\n",
  "response" : "HTTP/1.1 200 OK\nTransfer-Encoding: chunked\nConnection: keep-alive\nContent-Type: application/json\nDate: Mon, 03 Aug 2020 02:51:22 GMT\nServer: api-gateway\nX-Apig-Latency: 0\nX-Apig-Ratelimit-Api: remain:99,limit:100,time:1 minute\nX-Apig-Ratelimit-Api-Allenv: remain:14999,limit:15000,time:1 second\nX-Request-Id: d4ec6e33148bdeffe8f55b43472d1251\n\nmock success",
  "latency" : 5,
  "log" : ""
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:mode. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
}
```

```
{
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "API 3a955b791bd24b1c9cd94c745f8d1aad does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.5.9 Publishing APIs or Taking APIs Offline

Function

This API is used to publish multiple APIs in an environment or to remove multiple APIs from the environment in which they have been published.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/apis/publish

Table 4-307 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-308 Query Parameters

Parameter	Mandatory	Type	Description
action	Yes	String	• online: publish APIs • offline: take APIs offline

Request Parameters

Table 4-309 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-310 Request body parameters

Parameter	Mandatory	Type	Description
apis	No	Array of strings	IDs of APIs to be published or taken offline. A maximum of 1000 APIs are allowed at a time. Either apis or group_id must be specified.
env_id	Yes	String	Environment ID.
group_id	No	String	API group ID. Either apis or group_id must be specified.

Parameter	Mandatory	Type	Description
remark	No	String	Description of the publication. It cannot exceed 255 characters.

Response Parameters

Status code: 200

Table 4-311 Response body parameters

Parameter	Type	Description
success	Array of PublishResp objects	Message for successful API publication or taking offline.
failure	Array of BatchFailure objects	Error message and APIs that fail to be published or taken offline.

Table 4-312 PublishResp

Parameter	Type	Description
publish_id	String	Publication record ID.
api_id	String	API ID.
api_name	String	API name.
env_id	String	ID of the environment in which the API has been published.
remark	String	Description about the publication.
publish_time	String	Publication time.
version_id	String	API version currently in use.

Table 4-313 BatchFailure

Parameter	Type	Description
api_id	String	ID of an API that fails to be published or taken offline.
api_name	String	Name of an API that fails to be published or taken offline.

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 400**Table 4-314** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-315** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-316** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-317** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Publishing APIs

```
{
  "apis" : [ "3a955b791bd24b1c9cd94c745f8d1aad", "abd9c4b2ff974888b0ba79be7e6b2762" ],
  "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "remark" : "Published to the production environment"
}
```

Example Responses

Status code: 200

OK

```
{
  "success" : [ {
    "publish_id" : "9f27d1dc4f4242a9abf88e563dbfc33d",
    "api_id" : "3a955b791bd24b1c9cd94c745f8d1aad",
    "api_name" : "Api_mock",
    "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "version_id" : "632b2c9e022941969af9a1d45735ae2c",
    "remark" : "Published to the production environment",
    "publish_time" : "2020-08-03T03:01:31.26522821Z"
  } ],
  "failure" : [ {
    "api_id" : "abd9c4b2ff974888b0ba79be7e6b2762",
    "error_code" : "APIG.3002",
    "error_msg" : "Api abd9c4b2ff974888b0ba79be7e6b2762 not found"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value: parameter action should be \\\"online\\\" or \\\"offline\\\""
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
}
```

```
"error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.5.10 Querying Historical Versions of an API

Function

This API is used to query the historical versions of an API. APIG retains a maximum of 10 historical versions for each API in an environment.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apis/publish/{api_id}

Table 4-318 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
api_id	Yes	String	API ID.

Table 4-319 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
env_id	No	String	Environment ID.
env_name	No	String	Environment name.

Request Parameters

Table 4-320 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-321 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.

Parameter	Type	Description
api_versions	Array of ApiVersionResp objects	Historical version list.

Table 4-322 ApiVersionResp

Parameter	Type	Description
version_id	String	API version ID.
version_no	String	API version.
api_id	String	API ID.
env_id	String	ID of the environment in which the API has been published.
env_name	String	Name of the environment in which the API has been published.
remark	String	Description about the publication.
publish_time	String	Publication time.
status	Integer	Version status. • 1: effective • 2: not effective

Status code: 400**Table 4-323** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-324** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-325** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-326** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-327** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "api_versions" : [ {
    "version_id" : "ee1a5a38d3d3493abf1dc4ed6cacfa0b",
    "version_no" : "20200803093600",
    "api_id" : "5f918d104dc84480a75166ba99efff21",
    "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "env_name" : "RELEASE",
    "publish_time" : "2020-08-03T01:36:00Z",
    "status" : 1
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:env_name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "API 5f918d104dc84480a75166ba99efff21 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.5.11 Switching the Version of an API

Function

This API is used to switch the version of an API. A version is generated based on the current definition of an API when the API is published. The version records the definition and status of the API when it is published.

You can switch between multiple versions of an API, but only one version of an API takes effect in the same environment.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/apis/publish/{api_id}

Table 4-328 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
api_id	Yes	String	API ID.

Request Parameters

Table 4-329 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-330 Request body parameters

Parameter	Mandatory	Type	Description
version_id	No	String	API version ID.

Response Parameters

Status code: 200

Table 4-331 Response body parameters

Parameter	Type	Description
publish_id	String	Publication record ID.
api_id	String	API ID.
api_name	String	API name.
env_id	String	ID of the environment in which the API has been published.
remark	String	Description about the publication.
publish_time	String	Publication time.
version_id	String	API version currently in use.

Status code: 400

Table 4-332 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-333 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-334** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-335** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-336** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Switching an API to a specified version

```
{
  "version_id" : "ee1a5a38d3d3493abf1dc4ed6cacfa0b"
}
```

Example Responses

Status code: 200

OK

```
{
  "publish_id" : "9191cdb430724d4b8586ed7f1b962ca2",
  "api_id" : "5f918d104dc84480a75166ba99efff21",
  "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "version_id" : "ee1a5a38d3d3493abf1dc4ed6cacfa0b",
  "publish_time" : "2020-08-03T03:27:49.483295655Z"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2000",
  "error_msg" : "Parameter error: Serialization error: unexpected end of JSON input"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3022",
  "error_msg" : "The API version does not exist,id:ee1a5a38d3d3493abf1dc4ed6cacfa0b"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.5.12 Querying the Runtime Definition of an API

Function

This API is used to query the runtime definition of an API in a specified environment. The runtime definition of an API in the RELEASE environment is queried if no environment is specified.

The definition of an API is classified into the following types:

- Temporary definition: definition of an API used after the API was last edited.
- Runtime definition: snapshot of the temporary definition of an API captured when the API is published in an environment.

The runtime definition of an API is accessed when the API is called in an environment.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apis/runtime/{api_id}

Table 4-337 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
api_id	Yes	String	API ID.

Table 4-338 Query Parameters

Parameter	Mandatory	Type	Description
env_id	No	String	ID of the environment in which the API is published.

Request Parameters

Table 4-339 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-340** Response body parameters

Parameter	Type	Description
name	String	API name. It can contain 3 to 255 characters, starting with a letter or digit. Only letters, digits, and these special characters are allowed: - _./:()
type	Integer	API type. 1: public API 2: private API
version	String	API version. Maximum: 16
req_protocol	String	API request protocol: - HTTP - HTTPS - BOTH: Both HTTP and HTTPS are supported. - GRPCS Default: HTTPS
req_method	String	API request method. If the request protocol is set to GRPCS, the request method is fixed to POST.

Parameter	Type	Description
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. NOTE The address must comply with the URI specifications.
auth_type	String	API authentication mode. Options: • NONE • APP • IAM • AUTHORIZER: custom authentication. When auth_type is set to AUTHORIZER, the authorizer_id field is mandatory.
auth_opt	AuthOpt object	Security authentication parameter.
cors	Boolean	Indicates whether CORS is supported. • TRUE: supported • FALSE: not supported Default: false
trace_enabled	Boolean	Whether to enable tracing. By default, it is disabled. Default: false
sampling_strategy	String	Sampling policy. This parameter is mandatory when tracing is enabled. • RATE: sampling by percentage

Parameter	Type	Description
sampling_param	String	Sampling parameter. When sampling by percentage, the value of this parameter is an integer ranging from 0 to 100. The default value is 100, which indicates all requests are sampled. It is recommended that align the value with the backend sampling percentage. Default: 100 Minimum: 1 Maximum: 64
match_mode	String	API matching mode: - SWA: Prefix match - NORMAL: Exact match Default value: NORMAL
backend_type	String	Backend type. Options: - HTTP: web backend - FUNCTION: FunctionGraph backend. When backend_type is set to FUNCTION, the func_info field is mandatory. - MOCK: mock backend. When backend_type is set to MOCK, the mock_info field is mandatory. - GRPC: gRPC backend.
remark	String	API description. It cannot exceed 255 characters.
group_id	String	ID of the API group to which the API belongs.
body_remark	String	API request body, which can be an example request body, media type, or parameters. Ensure that the request body does not exceed 20,480 characters.
result_normal_sample	String	Example response for a successful request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.

Parameter	Type	Description
result_failure_sample	String	Example response for a failed request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.
authorizer_id	String	ID of the frontend custom authorizer
tags	Array of strings	Tag. Use letters, digits, and special characters (-*#%.:_) and start with a letter. By default, 10 tags are supported. To increase the quota, contact technical support to modify the API_TAG_NUM_LIMIT configuration. Minimum: 1 Maximum: 128
response_id	String	Group response ID.
roma_app_id	String	Integration application ID. Currently, this parameter is not supported.
domain_name	String	Custom domain name bound to the API. Currently, this parameter is not supported.
tag	String	Tag. This field will be deprecated. You can use the tags field instead.
content_type	String	Request content type: application/json application/xml multipart/form-data text/plain

Parameter	Type	Description
is_send_fg_body_base64	Boolean	Specifies whether to perform Base64 encoding on the body for interaction with FunctionGraph. The body does not need to be encoded using Base64 only when content_type is set to application/json. Application scenario: • Custom authentication • Bound circuit breaker plug-in with FunctionGraph backend downgrade policy • APIs with FunctionGraph backend Default: true
id	String	API ID.
group_name	String	Name of the API group to which the API belongs.
run_env_name	String	Name of the environment in which the API has been published.
run_env_id	String	ID of the environment in which the API has been published.
publish_id	String	Publication record ID.
sl_domain	String	Subdomain name of the API group.
sl_domains	Array of strings	Subdomain names that APIG automatically allocates to the API group.
req_params	Array of ReqParam objects	Request parameters.

Table 4-341 AuthOpt

Parameter	Type	Description
app_code_auth_type	String	Indicates whether AppCode authentication is enabled. This parameter is valid only if auth_type is set to App. The default value is DISABLE. - DISABLE: AppCode authentication is disabled. - HEADER: AppCode authentication is enabled and the AppCode is located in the header. Default: DISABLE

Table 4-342 ReqParam

Parameter	Type	Description
name	String	Parameter name. The parameter name can contain 1 to 32 characters and must start with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
type	String	Parameter type.
location	String	Parameter location.
default_value	String	Default value.
sample_value	String	Example value.
required	Integer	Indicates whether the parameter is required. 1: yes 2: no The value of this parameter is 1 if Location is set to PATH, and 2 if Location is set to another value.
valid_enable	Integer	Indicates whether validity check is enabled. 1: enabled 2: disabled Default: 2

Parameter	Type	Description
remark	String	Description. It cannot exceed 255 characters.
enumerations	String	Enumerated value.
min_num	Integer	Minimum value. This parameter is valid when type is set to NUMBER.
max_num	Integer	Maximum value. This parameter is valid when type is set to NUMBER.
min_size	Integer	Minimum length. This parameter is valid when type is set to STRING.
max_size	Integer	Maximum length. This parameter is valid when type is set to STRING.
regular	String	Regular expression validation rule. Currently, this parameter is not supported.
json_schema	String	JSON validation rule. Currently, this parameter is not supported.
pass_through	Integer	Indicates whether to transparently transfer the parameter. 1: yes 2: no

Parameter	Type	Description
orchestrations	Array of strings	Request parameter orchestration rules are prioritized in the same sequence as the list. The none_value rule in a rule list has the highest priority. A maximum of one none_value rule can be bound. The default rule in a rule list has the lowest priority. A maximum of one default rule can be bound. The preprocessing orchestration rule cannot be used as the last orchestration rule except the default rule. Only one parameter of each API can be bound with unique orchestration rules. The number of orchestration rules that can be bound is limited by quota. For details, see "Notes and Constraints" in APIG Service Overview.
id	String	Parameter ID.

Status code: 401**Table 4-343** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-344** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-345 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-346 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "name" : "Api_http",
  "type" : 1,
  "version" : "V0.0.1",
  "req_protocol" : "HTTPS",
  "req_method" : "GET",
  "req_uri" : "/test/http",
  "auth_type" : "AUTHORIZER",
  "authorizer_id" : "8d0443832a194eaa84244e0c1c1912ac",
  "auth_opt" : {
    "app_code_auth_type" : "DISABLE"
  },
  "cors" : false,
  "match_mode" : "NORMAL",
  "backend_type" : "HTTP",
  "remark" : "Web backend API",
  "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "result_normal_sample" : "Example success response",
  "result_failure_sample" : "Example failure response",
  "id" : "5f918d104dc84480a75166ba99efff21",
  "group_name" : "api_group_001",
  "run_env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "run_env_name" : "RELEASE",
  "publish_id" : "9191cdb430724d4b8586ed7f1b962ca2",
  "sl_domain" : "c77f5e81d9cb4424bf704ef2b0ac7600.apic.***.com",
  "sl_domains" : [ "c77f5e81d9cb4424bf704ef2b0ac7600.apic.***.com",
    "c77f5e81d9cb4424bf704ef2b0ac7600.apic.***.cn" ]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "API 5f918d104dc84480a75166ba99efff21 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.5.13 Querying API Version Details

Function

This API is used to query the details of a specified API version.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apis/versions/{version_id}

Table 4-347 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
version_id	Yes	String	API version.

Request Parameters

Table 4-348 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-349 Response body parameters

Parameter	Type	Description
name	String	API name. It can contain 3 to 255 characters, starting with a letter or digit. Only letters, digits, and these special characters are allowed: -_./:()

Parameter	Type	Description
type	Integer	API type. 1: public API 2: private API
version	String	API version. Maximum: 16
req_protocol	String	API request protocol: - HTTP - HTTPS - BOTH: Both HTTP and HTTPS are supported. - GRPCS Default: HTTPS
req_method	String	API request method. If the request protocol is set to GRPCS, the request method is fixed to POST.
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. NOTE The address must comply with the URI specifications.
auth_type	String	API authentication mode. Options: - NONE - APP - IAM - AUTHORIZER: custom authentication. When auth_type is set to AUTHORIZER, the authorizer_id field is mandatory.
auth_opt	AuthOpt object	Security authentication parameter.
cors	Boolean	Indicates whether CORS is supported. - TRUE: supported - FALSE: not supported Default: false

Parameter	Type	Description
trace_enabled	Boolean	Whether to enable tracing. By default, it is disabled. Default: false
sampling_strategy	String	Sampling policy. This parameter is mandatory when tracing is enabled. • RATE: sampling by percentage
sampling_param	String	Sampling parameter. • When sampling by percentage, the value of this parameter is an integer ranging from 0 to 100. The default value is 100, which indicates all requests are sampled. It is recommended that align the value with the backend sampling percentage. Default: 100 Minimum: 1 Maximum: 64
match_mode	String	API matching mode: • SWA: Prefix match • NORMAL: Exact match Default value: NORMAL
backend_type	String	Backend type. Options: • HTTP: web backend • FUNCTION: FunctionGraph backend. When backend_type is set to FUNCTION, the func_info field is mandatory. • MOCK: mock backend. When backend_type is set to MOCK, the mock_info field is mandatory. • GRPC: gRPC backend.
remark	String	API description. It cannot exceed 255 characters.
group_id	String	ID of the API group to which the API belongs.
body_remark	String	API request body, which can be an example request body, media type, or parameters. Ensure that the request body does not exceed 20,480 characters.

Parameter	Type	Description
result_normal_sample	String	Example response for a successful request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.
result_failure_sample	String	Example response for a failed request. Ensure that the response does not exceed 20,480 characters. This is unavailable if the request protocol is set to GRPC.
authorizer_id	String	ID of the frontend custom authorizer
tags	Array of strings	Tag. Use letters, digits, and special characters (-*#%.:_) and start with a letter. By default, 10 tags are supported. To increase the quota, contact technical support to modify the API_TAG_NUM_LIMIT configuration. Minimum: 1 Maximum: 128
response_id	String	Group response ID.
roma_app_id	String	Integration application ID. Currently, this parameter is not supported.
domain_name	String	Custom domain name bound to the API. Currently, this parameter is not supported.
tag	String	Tag. This field will be deprecated. You can use the tags field instead.
content_type	String	Request content type: application/json application/xml multipart/form-data text/plain

Parameter	Type	Description
is_send_fg_body_base64	Boolean	Specifies whether to perform Base64 encoding on the body for interaction with FunctionGraph. The body does not need to be encoded using Base64 only when content_type is set to application/json. Application scenario: • Custom authentication • Bound circuit breaker plug-in with FunctionGraph backend downgrade policy • APIs with FunctionGraph backend Default: true
id	String	API ID.
status	Integer	App status. • 1: valid
arrange_necessary	Integer	Indicates whether to enable orchestration.
register_time	String	Time when the API is registered.
update_time	String	Time when the API was last modified.
group_name	String	Name of the API group to which the API belongs.
group_version	String	Version of the API group to which the API belongs. The default value is V1. Other versions are not supported. Default: V1
run_env_id	String	ID of the environment in which the API has been published. Separate multiple environment IDs with vertical bars ().
run_env_name	String	Name of the environment in which the API has been published. Separate multiple environment names with vertical bars ().
publish_id	String	Publication record ID. Separate multiple publication record IDs with vertical bars ().

Parameter	Type	Description
publish_time	String	Time when the API version is published.
roma_app_name	String	Name of the integration application to which the API belongs. Currently, this parameter is not supported.
ld_api_id	String	ID of the corresponding custom backend API. Currently, this parameter is not supported.
backend_api	BackendApi object	Web backend details.
api_group_info	ApiGroupCommonInfo object	API group information.
func_info	ApiFunc object	FunctionGraph backend details.
mock_info	ApiMock object	Mock backend details.
req_params	Array of ReqParam objects	Request parameters.
backend_params	Array of BackendParam objects	Backend parameters.
policy_functions	Array of ApiPolicyFunctionResp objects	FunctionGraph backend policies.
policy_mocks	Array of ApiPolicyMockResp objects	Mock backend policies.
policy_https	Array of ApiPolicyHttpResp objects	Web backend policies.
sl_domain	String	Subdomain name that API Gateway automatically allocates to the API group.
sl_domains	Array of strings	Subdomain names that APIG automatically allocates to the API group.
version_id	String	API version ID.

Table 4-350 AuthOpt

Parameter	Type	Description
app_code_auth_type	String	Indicates whether AppCode authentication is enabled. This parameter is valid only if auth_type is set to App. The default value is DISABLE. - DISABLE: AppCode authentication is disabled. - HEADER: AppCode authentication is enabled and the AppCode is located in the header. Default: DISABLE

Table 4-351 BackendApi

Parameter	Type	Description
authorizer_id	String	Backend custom authorizer ID.
url_domain	String	Address of the backend service. This parameter is required when no VPC channel is used. It consists of a domain name or IP address and a port number. Maximum length: 255 characters. It must be in the format "Host name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
req_protocol	String	Request protocol. You can select GRPC or GRPCS for the GRPC backend.
remark	String	Description. It cannot exceed 255 characters.
req_method	String	Request method. For the GRPC backend, the request method is fixed to POST.
version	String	Web backend version, which can contain a maximum of 16 characters.

Parameter	Type	Description
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications. For the GRPC backend, the request address is fixed to /.
timeout	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms. Minimum: 1
enable_client_ssl	Boolean	Indicates whether to enable two-way authentication.
retry_count	String	Number of retry attempts to request the backend service. The default value is -1. The value ranges from -1 to 10. -1 indicates that idempotent APIs will retry once and non-idempotent APIs will not retry. POST and PATCH are non-idempotent. GET, HEAD, PUT, OPTIONS, and DELETE are idempotent. Default: -1
enable_sm_channel	Boolean	Indicates whether to enable SM cryptographic algorithms. This feature is only available if the gateway supports the SM cryptographic algorithms.
id	String	ID.

Parameter	Type	Description
status	Integer	Backend service status. 1: valid
register_time	String	Registration time.
update_time	String	Update time.
vpc_channel_info	VpcInfo object	VPC channel details. This parameter is required if vpc_channel_status is set to 1.
vpc_channel_status	Integer	Indicates whether to use a VPC channel. 1: A VPC channel is used. 2: No VPC channel is used.

Table 4-352 ApiGroupCommonInfo

Parameter	Type	Description
id	String	ID.
name	String	API group name.
status	Integer	Status. 1: valid
sl_domain	String	Subdomain name that APIG automatically allocates to the API group.
register_time	String	Creation time.
update_time	String	Last modification time.
on_sell_status	Integer	Indicates whether the API group has been listed on KooGallery. 1: listed 2: not listed 3: under review Not supported currently.
url_domains	Array of UrlDomain objects	Independent domain names bound to the API group.
sl_domain_access_enabled	Boolean	Whether the debugging domain name is accessible. Options: true and false. Default: true

Table 4-353 UrlDomain

Parameter	Type	Description
id	String	Domain ID.
domain	String	Domain name.
cname_status	Integer	CNAME resolution status of the domain name. • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
min_ssl_version	String	Minimum SSL version. TLS 1.1 and TLS 1.2 are supported. Default: TLSv1.1
verified_client_certificate_enabled	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false
is_has_trusted_root_ca	Boolean	Whether a trusted root certificate (CA) exists. The value is true if trusted_root_ca exists in the bound certificate. Default: false

Parameter	Type	Description
ingress_http_port	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ingress_https_port	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ssl_infos	Array of SslInfo objects	SSL certificate list.

Table 4-354 SslInfo

Parameter	Type	Description
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2
type	String	Certificate scope: • instance • global Default: global

Table 4-355 ApiFunc

Parameter	Type	Description
function_urn	String	Function URN.
remark	String	Description. It cannot exceed 255 characters.
invocation_type	String	Invocation mode. • async: asynchronous • sync: synchronous
network_type	String	Function network architecture. • V1: non-VPC • V2: VPC
version	String	Function version. If both a function alias URN and version are passed, only the alias URN will be used. Maximum: 64
alias_urn	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.

Parameter	Type	Description
timeout	Integer	Timeout allowed for APIG to request the backend service. If the function network architecture is set to V1, the maximum timeout is 60,000. If the network architecture is set to V2, the maximum timeout is 600,000 and can be modified by using the gateway parameter backend_timeout. Unit: ms. Minimum: 1
authorizer_id	String	Backend custom authorizer ID.
req_protocol	String	Backend request protocol of a function. The value can be HTTPS (default) or GRPCS (available when the frontend request protocol is GRPCS). Default: HTTPS
id	String	ID.
register_time	String	Registration time.
status	Integer	Backend service status. • 1: valid
update_time	String	Update time.

Table 4-356 ApiMock

Parameter	Type	Description
remark	String	Description. It cannot exceed 255 characters.
result_content	String	Response.
version	String	Function version. It cannot exceed 64 characters.
authorizer_id	String	Backend custom authorizer ID.
id	String	ID.
register_time	String	Registration time.
status	Integer	Backend service status. • 1: valid
update_time	String	Update time.

Table 4-357 ReqParam

Parameter	Type	Description
name	String	Parameter name. The parameter name can contain 1 to 32 characters and must start with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
type	String	Parameter type.
location	String	Parameter location.
default_value	String	Default value.
sample_value	String	Example value.
required	Integer	Indicates whether the parameter is required. 1: yes 2: no The value of this parameter is 1 if Location is set to PATH, and 2 if Location is set to another value.
valid_enable	Integer	Indicates whether validity check is enabled. 1: enabled 2: disabled Default: 2
remark	String	Description. It cannot exceed 255 characters.
enumerations	String	Enumerated value.
min_num	Integer	Minimum value. This parameter is valid when type is set to NUMBER.
max_num	Integer	Maximum value. This parameter is valid when type is set to NUMBER.
min_size	Integer	Minimum length. This parameter is valid when type is set to STRING.
max_size	Integer	Maximum length. This parameter is valid when type is set to STRING.

Parameter	Type	Description
regular	String	Regular expression validation rule. Currently, this parameter is not supported.
json_schema	String	JSON validation rule. Currently, this parameter is not supported.
pass_through	Integer	Indicates whether to transparently transfer the parameter. 1: yes 2: no
orchestrations	Array of strings	Request parameter orchestration rules are prioritized in the same sequence as the list. The none_value rule in a rule list has the highest priority. A maximum of one none_value rule can be bound. The default rule in a rule list has the lowest priority. A maximum of one default rule can be bound. The preprocessing orchestration rule cannot be used as the last orchestration rule except the default rule. Only one parameter of each API can be bound with unique orchestration rules. The number of orchestration rules that can be bound is limited by quota. For details, see "Notes and Constraints" in APIG Service Overview.
id	String	Parameter ID.

Table 4-358 ApiPolicyFunctionResp

Parameter	Type	Description
function_urn	String	Function URN.
invocation_type	String	Invocation mode. • async: asynchronous • sync: synchronous

Parameter	Type	Description
network_type	String	Function network architecture. • V1: non-VPC • V2: VPC
version	String	Function version. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored. Maximum: 64
alias_urn	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
timeout	Integer	Timeout allowed for APIG to request the backend service. If the function network architecture is set to V1, the maximum timeout is 60,000. If the network architecture is set to V2, the maximum timeout is 600,000 and can be modified by using the gateway parameter backend_timeout. Unit: ms. Minimum: 1
req_protocol	String	Backend request protocol of a function. The value can be HTTPS (default) or GRPCS (available when the frontend request protocol is GRPCS). Default: HTTPS
id	String	ID.
effect_mode	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	String	Backend name, which must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64

Parameter	Type	Description
backend_params	Array of BackendParam objects	Backend parameters.
conditions	Array of CoditionResp objects	Policy conditions.
authorizer_id	String	Backend custom authorizer ID.

Table 4-359 ApiPolicyMockResp

Parameter	Type	Description
id	String	ID.
effect_mode	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.
name	String	Backend name, which must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_params	Array of BackendParam objects	Backend parameters.
conditions	Array of CoditionResp objects	Policy conditions.
authorizer_id	String	Backend custom authorizer ID.
result_content	String	Response.

Table 4-360 ApiPolicyHttpResp

Parameter	Type	Description
id	String	ID.
effect_mode	String	Effective mode of the backend policy. • ALL: All conditions are met. • ANY: Any condition is met.

Parameter	Type	Description
name	String	Backend name, which must start with a letter and can contain letters, digits, and underscores (_). Minimum: 3 Maximum: 64
backend_params	Array of BackendParam objects	Backend parameters.
conditions	Array of CoditionResp objects	Policy conditions.
authorizer_id	String	Backend custom authorizer ID.
url_domain	String	Endpoint of the policy backend. An endpoint consists of a domain name or IP address and a port number, with not more than 255 characters. It must be in the format "Domain name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
req_protocol	String	Request protocol. Options include HTTP, HTTPS, GRPC, or GRPCS. You can select GRPC or GRPCS for the GRPC backend.
req_method	String	Request method. Options include GET, POST, PUT, DELETE, HEAD, PATCH, OPTIONS, and ANY. This is fixed to POST for the GRPC backend.

Parameter	Type	Description
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications. For the GRPC backend, the request address is fixed to /.
timeout	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms. Minimum: 1
retry_count	String	Number of retry attempts to request the backend service. The default value is -1. The value ranges from -1 to 10. -1 indicates that idempotent APIs will retry once and non-idempotent APIs will not retry. POST and PATCH are non-idempotent. GET, HEAD, PUT, OPTIONS, and DELETE are idempotent. Default: -1
enable_sm_channel	Boolean	Indicates whether to enable SM cryptographic algorithms. This feature is only available if the gateway supports the SM cryptographic algorithms.
vpc_channel_info	VpcInfo object	VPC channel details. This parameter is required if vpc_channel_status is set to 1.

Parameter	Type	Description
vpc_channel_status	Integer	Indicates whether to use a VPC channel. • 1: A VPC channel is used. • 2: No VPC channel is used.

Table 4-361 BackendParam

Parameter	Type	Description
origin	String	Parameter type. • REQUEST: backend parameter • CONSTANT: constant parameter • SYSTEM: system parameter
name	String	Parameter name. The parameter name must start with a letter and can only contain letters, digits, hyphens (-), underscores (_), and periods (.). Minimum: 1 Maximum: 32
remark	String	Description, which can contain a maximum of 255 characters.
location	String	Parameter location. The value can be PATH, QUERY, or HEADER.

Parameter	Type	Description
value	String	Parameter value, which can contain a maximum of 255 characters. If the origin type is REQUEST, the value of this parameter is the parameter name in req_params. If the origin type is CONSTANT, the value is a constant. If the origin type is SYSTEM, the value is a system parameter name. System parameters include gateway parameters, frontend authentication parameters, and backend authentication parameters. You can set the frontend or backend authentication parameters after enabling custom frontend or backend authentication. The gateway parameters are as follows: • \$context.sourceIp: source IP address of the API caller. • \$context.stage: deployment environment in which the API is called. • \$context.apid: API ID. • \$context.appId: ID of the app used by the API caller. • \$context.requestId: request ID generated when the API is called. • \$context.serverAddr: address of the gateway server. • \$context.serverName: name of the gateway server. • \$context.handleTime: time when the API request is processed. • \$context.providerAppId: ID of the app used by the API owner. This parameter is currently not supported. Frontend authentication parameter: prefixed with "\$context.authorizer.frontend.". For example, to return "aaa" upon successful custom authentication, set this parameter to "\$context.authorizer.frontend.aaa".

Parameter	Type	Description
		Backend authentication parameter: prefixed with "\$context.authorizer.backend.". For example, to return "aaa" upon successful custom authentication, set this parameter to "\$context.authorizer.backend.aaa".
id	String	Parameter ID.
req_param_id	String	Request parameter ID.

Table 4-362 CoditionResp

Parameter	Type	Description
req_param_name	String	Input parameter name. This parameter is required if the policy type is param.
sys_param_name	String	Name of a built-in gateway parameter. This parameter is required if the policy type is system. The following parameters are supported: - req_path: request path. For example, /a/b. - req_method: request method. For example, GET. - reqPath: request path, which is discarded. For example, /a/b. - reqMethod: request method, which is discarded. For example, GET.
cookie_param_name	String	COOKIE parameter name. This parameter is required if the policy type is cookie. Minimum: 0 Maximum: 255

Parameter	Type	Description
frontend_authorizer_param_name	String	System parameter: frontend authentication parameter name. This parameter is mandatory when the policy type is frontend_authorizer. The frontend authentication parameter name is prefixed with \$context.authorizer.frontend. For example, if the frontend authentication parameter name is user_name, the name with the prefix will be \$context.authorizer.frontend.user_name.
condition_type	String	Policy condition. • exact: Exact match • enum: Enumeration • pattern: Regular expression This parameter is required when the policy type is param, system, cookie, or frontend_authorizer.
condition_origin	String	Policy type • param: parameter • source: source IP address • system: system parameter - gateway built-in parameter • cookie: COOKIE parameter • frontend_authorizer: system parameter - frontend authentication parameter
condition_value	String	Policy value. Maximum: 1024
mapped_param_name	String	Name of a parameter generated after orchestration. This parameter is mandatory when condition_origin is set to orchestration. The generated parameter name must exist in the orchestration rule bound to the API.
mapped_param_location	String	Location of a parameter generated after orchestration. This parameter is mandatory when condition_origin is set to orchestration. This location must exist in the orchestration rule bound to the API.

Parameter	Type	Description
id	String	ID.
req_param_id	String	Input parameter ID.
req_param_location	String	Input parameter location.

Table 4-363 VpcInfo

Parameter	Type	Description
ecs_id	String	Cloud server ID.
ecs_name	String	Cloud server name.
cascade_flag	Boolean	Indicates whether to use the cascading mode. Currently, this parameter is not supported.
vpc_channel_proxy_host	String	Proxy host.
vpc_channel_id	String	VPC channel ID.
vpc_channel_port	Integer	VPC channel port.

Status code: 401**Table 4-364** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-365** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-366** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-367** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "name" : "Api_http",
  "type" : 1,
  "version" : "V0.0.1",
  "req_protocol" : "HTTPS",
  "req_method" : "GET",
  "req_uri" : "/test/http",
  "auth_type" : "AUTHORIZER",
  "auth_opt" : [ {
    "app_code_auth_type" : "DISABLE"
  } ],
  "authorizer_id" : "8d0443832a194eaa84244e0c1c1912ac",
  "cors" : false,
  "trace_enabled" : true,
  "sampling_strategy" : "RATE",
  "sampling_param" : "10",
  "match_mode" : "NORMAL",
  "backend_type" : "HTTP",
  "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "result_normal_sample" : "Example success response",
  "result_failure_sample" : "Example failure response",
  "id" : "5f918d104dc84480a75166ba99efff21",
  "status" : 1,
  "arrange_necessary" : 2,
  "remark" : "Web backend API",
  "register_time" : "2020-07-31T12:42:51Z",
  "update_time" : "2020-08-02T16:32:47.046289Z",
  "group_name" : "api_group_001",
}
```

```
"run_env_name" : "RELEASE",
"run_env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
"sl_domain" : "c77f5e81d9cb4424bf704ef2b0ac7600.apic.***.com",
"sl_domains" : [ "c77f5e81d9cb4424bf704ef2b0ac7600.apic.***.com",
"c77f5e81d9cb4424bf704ef2b0ac7600.apic.***.cn" ],
"version_id" : "ee1a5a38d3d3493abf1dc4ed6cacfa0b",
"publish_time" : "2020-08-03T01:36:00Z",
"backend_api" : {
  "url_domain" : "56a7d7358e1b42459c9d730d65b14e59",
  "req_protocol" : "HTTPS",
  "req_method" : "GET",
  "req_uri" : "/test/benchmark",
  "timeout" : 5000,
  "id" : "1ce8fda3586d4371bd83c955df37e102",
  "status" : 1,
  "register_time" : "2020-07-31T12:42:51Z",
  "update_time" : "2020-08-02T16:32:47.077029Z",
  "vpc_channel_status" : 1,
  "vpc_channel_info" : {
    "cascade_flag" : false,
    "vpc_channel_id" : "56a7d7358e1b42459c9d730d65b14e59",
    "vpc_channel_proxy_host" : "www.example.com",
    "vpc_channel_port" : 0
  },
  "retry_count" : "-1"
},
"backend_params" : [ {
  "name" : "X-CONSTANT-HEADER",
  "location" : "HEADER",
  "origin" : "CONSTANT",
  "value" : "demo",
  "remark" : "constant_demo",
  "id" : "8cb2eba19e7a4423a4e835647a8b8d76"
}, {
  "name" : "app-id",
  "location" : "HEADER",
  "origin" : "SYSTEM",
  "value" : "$context.appld",
  "remark" : "App ID of the API caller",
  "id" : "216ddda836e74d528f364ff589d9dd21"
} ]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3022",
  "error_msg" : "The API version does not exist,id:ee1a5a38d3d3493abf1dc4ed6cacfa0b"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.5.14 Taking an API Version Offline

Function

This API is used to remove an effective version of an API. The removed API cannot be called in the environment in which it took effect.

Calling MethodFor details, see [Calling APIs](#).**URI**

DELETE /v2/{project_id}/apigw/instances/{instance_id}/apis/versions/{version_id}

Table 4-368 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
version_id	Yes	String	API version.

Request Parameters

Table 4-369 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 401

Table 4-370 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-371 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-372 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-373 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3022",
  "error_msg" : "The API version does not exist,id:ee1a5a38d3d3493abf1dc4ed6cacfa0b"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
}
```



```
"error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.6 Signature Key Management

4.6.1 Creating a Signature Key

Function

It is a good practice to provide a protection mechanism for APIs to ensure access security. For example, authenticating API request sources and denying the access from unauthorized sources.

A signature key is a protection mechanism in case.

Create a signature key and bind it to an API. When requesting the API, APIG uses the signature key to encrypt request parameter data and generate a signature. The backend service of the API verifies requests by using the signature. Unauthorized requests will be denied to protect the API against attacks from unknown sources.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/signs

Table 4-374 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-375 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-376 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Signature key name. It can contain letters, digits, and underscores(_) and must start with a letter. Minimum: 3 Maximum: 64

Parameter	Mandatory	Type	Description
sign_type	No	String	Signature key type: • hmac -basic -public_key -aes To use a basic signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway. To use a public_key signature key, ensure that the public_key feature has been configured for your gateway. For details, see "Appendix" > "Supported Features". If your gateway does not support this feature, contact technical support to enable it. To use an AES signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway.

Parameter	Mandatory	Type	Description
sign_key	No	String	Signature key. • hmac: The value contains 8 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter or digit. If not specified, a key is automatically generated. • basic: The value contains 4 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter. If not specified, a key is automatically generated. • public_key: The value contains 8 to 512 characters, including letters, digits, and special characters (_-+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated. • aes: The value contains 16 characters if the aes-128-cfb algorithm is used, or 32 characters if the aes-256-cfb algorithm is used. Letters, digits, and special characters (_-!@#%+/=) are allowed. It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated.

Parameter	Mandatory	Type	Description
sign_secret	No	String	Signature secret. • hmac: The value contains 16 to 64 characters. Letters, digits, and special characters (_-!@\$%) are allowed. It must start with a letter or digit. If not specified, a key is automatically generated. • basic: The value contains 8 to 64 characters. Letters, digits, and special characters (_-!@\$%) are allowed. It must start with a letter or digit. If not specified, a key is automatically generated. • public_key: The value can contain 16 to 2048 characters, including letters, digits, and special characters (_-!@\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated. • aes: The value contains 16 characters, including letters, digits, and special characters (_-!@\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated.
sign_algorithm	No	String	Signature algorithm. Specify a signature algorithm only when using an AES signature key. By default, no algorithm is used.

Response Parameters

Status code: 201

Table 4-377 Response body parameters

Parameter	Type	Description
name	String	Signature key name. It can contain letters, digits, and underscores(_) and must start with a letter. Minimum: 3 Maximum: 64
sign_type	String	Signature key type: • hmac -basic -public_key -aes To use a basic signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway. To use a public_key signature key, ensure that the public_key feature has been configured for your gateway. For details, see "Appendix" > "Supported Features". If your gateway does not support this feature, contact technical support to enable it. To use an AES signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway.

Parameter	Type	Description
sign_key	String	Signature key. • hmac: The value contains 8 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter or digit. If not specified, a key is automatically generated. • basic: The value contains 4 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter. If not specified, a key is automatically generated. • public_key: The value contains 8 to 512 characters, including letters, digits, and special characters (_-+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated. • aes: The value contains 16 characters if the aes-128-cfb algorithm is used, or 32 characters if the aes-256-cfb algorithm is used. Letters, digits, and special characters (_-!@#\$%+/=) are allowed. It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated.

Parameter	Type	Description
sign_secret	String	Signature secret. • hmac: The value contains 16 to 64 characters. Letters, digits, and special characters (_-!@#\$%) are allowed. It must start with a letter or digit. If not specified, a key is automatically generated. • basic: The value contains 8 to 64 characters. Letters, digits, and special characters (_-!@#\$%) are allowed. It must start with a letter or digit. If not specified, a key is automatically generated. • public_key: The value can contain 16 to 2048 characters, including letters, digits, and special characters (_-!@#\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated. • aes: The value contains 16 characters, including letters, digits, and special characters (_-!@#\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated.
sign_algorithm	String	Signature algorithm. Specify a signature algorithm only when using an AES signature key. By default, no algorithm is used.
update_time	String	Update time.
create_time	String	Creation time.
id	String	Signature key ID.

Status code: 400

Table 4-378 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-379** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-380** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-381** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 412**Table 4-382** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-383** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Example Requests

Create a signature key with a custom key and secret.

```
{
  "name" : "signature_demo",
  "sign_key" : "signkeysignkey",
  "sign_secret" : "sig*****ret"
}
```

Example Responses

Status code: 201

Created

```
{
  "sign_secret" : "sig*****ret",
  "update_time" : "2020-08-03T03:39:38.119032888Z",
  "create_time" : "2020-08-03T03:39:38.119032659Z",
  "name" : "signature_demo",
  "id" : "0b0e8f456b8742218af75f945307173c",
  "sign_key" : "signkeysignkey",
  "sign_type" : "hmac"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
}
```

```
{
  "error_msg" : "The instance does not exist;id:f0fa1789-3b76-433b-a787-9892951c620ec"
}
```

Status code: 412

PreconditionFailed

```
{
  "error_code" : "APIG.3548",
  "error_msg" : "sign_type=public_key not supported by instance 6a29d4e9-69a0-412a-aabe-9898ec0903b0"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
412	PreconditionFailed
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.6.2 Modifying a Signature Key

Function

This API is used to modify the information about a signature key.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/signs/{sign_id}

Table 4-384 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
sign_id	Yes	String	Signature key ID.

Request Parameters

Table 4-385 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-386 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Signature key name. It can contain letters, digits, and underscores(_) and must start with a letter. Minimum: 3 Maximum: 64

Parameter	Mandatory	Type	Description
sign_type	No	String	Signature key type: • hmac -basic -public_key -aes To use a basic signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway. To use a public_key signature key, ensure that the public_key feature has been configured for your gateway. For details, see "Appendix" > "Supported Features". If your gateway does not support this feature, contact technical support to enable it. To use an AES signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway.

Parameter	Mandatory	Type	Description
sign_key	No	String	Signature key. • hmac: The value contains 8 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter or digit. If not specified, a key is automatically generated. • basic: The value contains 4 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter. If not specified, a key is automatically generated. • public_key: The value contains 8 to 512 characters, including letters, digits, and special characters (_-+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated. • aes: The value contains 16 characters if the aes-128-cfb algorithm is used, or 32 characters if the aes-256-cfb algorithm is used. Letters, digits, and special characters (_-!@#%+/=) are allowed. It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated.

Parameter	Mandatory	Type	Description
sign_secret	No	String	Signature secret. • hmac: The value contains 16 to 64 characters. Letters, digits, and special characters (_-!@\$%) are allowed. It must start with a letter or digit. If not specified, a key is automatically generated. • basic: The value contains 8 to 64 characters. Letters, digits, and special characters (_-!@\$%) are allowed. It must start with a letter or digit. If not specified, a key is automatically generated. • public_key: The value can contain 16 to 2048 characters, including letters, digits, and special characters (_-!@\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated. • aes: The value contains 16 characters, including letters, digits, and special characters (_-!@\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated.
sign_algorithm	No	String	Signature algorithm. Specify a signature algorithm only when using an AES signature key. By default, no algorithm is used.

Response Parameters

Status code: 200

Table 4-387 Response body parameters

Parameter	Type	Description
name	String	Signature key name. It can contain letters, digits, and underscores(_) and must start with a letter. Minimum: 3 Maximum: 64
sign_type	String	Signature key type: • hmac -basic -public_key -aes To use a basic signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway. To use a public_key signature key, ensure that the public_key feature has been configured for your gateway. For details, see "Appendix" > "Supported Features". If your gateway does not support this feature, contact technical support to enable it. To use an AES signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway.

Parameter	Type	Description
sign_key	String	Signature key. • hmac: The value contains 8 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter or digit. If not specified, a key is automatically generated. • basic: The value contains 4 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter. If not specified, a key is automatically generated. • public_key: The value contains 8 to 512 characters, including letters, digits, and special characters (_-+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated. • aes: The value contains 16 characters if the aes-128-cfb algorithm is used, or 32 characters if the aes-256-cfb algorithm is used. Letters, digits, and special characters (_-!@#\$%+/=) are allowed. It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated.

Parameter	Type	Description
sign_secret	String	Signature secret. • hmac: The value contains 16 to 64 characters. Letters, digits, and special characters (_-!@\$%) are allowed. It must start with a letter or digit. If not specified, a key is automatically generated. • basic: The value contains 8 to 64 characters. Letters, digits, and special characters (_-!@\$%) are allowed. It must start with a letter or digit. If not specified, a key is automatically generated. • public_key: The value can contain 16 to 2048 characters, including letters, digits, and special characters (_-!@\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated. • aes: The value contains 16 characters, including letters, digits, and special characters (_-!@\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated.
sign_algorithm	String	Signature algorithm. Specify a signature algorithm only when using an AES signature key. By default, no algorithm is used.
update_time	String	Update time.
create_time	String	Creation time.
id	String	Signature key ID.

Status code: 400

Table 4-388 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-389** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-390** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-391** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 412**Table 4-392** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-393** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Example Requests

Modify the name of a specified signature key.

```
{
  "name" : "signature_demo"
}
```

Example Responses

Status code: 200

OK

```
{
  "sign_secret" : "dc0*****2b3",
  "update_time" : "2020-08-03T03:50:14.989785802Z",
  "create_time" : "2020-08-03T03:39:38Z",
  "name" : "signature_demo",
  "id" : "0b0e8f456b8742218af75f945307173c",
  "sign_key" : "a071a20d460a4f639a636c3d7e3d8163",
  "sign_type" : "hmac"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3017",
  "error_msg" : "Signature key 0b0e8f456b8742218af75f945307173c does not exist"
}
```

Status code: 412

PreconditionFailed

```
{
  "error_code" : "APIG.3548",
  "error_msg" : "sign_type=public_key not supported by instance 6a29d4e9-69a0-412a-aabe-9898ec0903b0"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
412	PreconditionFailed
500	Internal Server Error

Error CodesSee [Error Codes](#).**4.6.3 Deleting a Signature Key****Function**

This API is used to delete a signature key. This operation will invalidate the signature key and unbind it from the APIs to which it was bound.

Calling MethodFor details, see [Calling APIs](#).**URI**

DELETE /v2/{project_id}/apigw/instances/{instance_id}/signs/{sign_id}

Table 4-394 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
sign_id	Yes	String	Signature key ID.

Request Parameters

Table 4-395 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 401

Table 4-396 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-397 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-398** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-399** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3017",
  "error_msg": "Signature key 0b0e8f456b8742218af75f945307173c does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
204	No Content
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.6.4 Querying Signature Keys

Function

This API is used to query all the signature keys.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/signs

Table 4-400 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-401 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
id	No	String	Signature key ID.
name	No	String	Signature key name.
precise_search	No	String	Parameter name (name) for exact matching.

Request Parameters

Table 4-402 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-403 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
signs	Array of SignatureWithBindNum objects	Signature key list.

Table 4-404 SignatureWithBindNum

Parameter	Type	Description
name	String	Signature key name. It can contain letters, digits, and underscores(_) and must start with a letter. Minimum: 3 Maximum: 64

Parameter	Type	Description
sign_type	String	Signature key type: • hmac -basic -public_key -aes To use a basic signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway. To use a public_key signature key, ensure that the public_key feature has been configured for your gateway. For details, see "Appendix" > "Supported Features". If your gateway does not support this feature, contact technical support to enable it. To use an AES signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway.

Parameter	Type	Description
sign_key	String	Signature key. • hmac: The value contains 8 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter or digit. If not specified, a key is automatically generated. • basic: The value contains 4 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter. If not specified, a key is automatically generated. • public_key: The value contains 8 to 512 characters, including letters, digits, and special characters (_-+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated. • aes: The value contains 16 characters if the aes-128-cfb algorithm is used, or 32 characters if the aes-256-cfb algorithm is used. Letters, digits, and special characters (_-!@#\$%+/=) are allowed. It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated.

Parameter	Type	Description
sign_secret	String	Signature secret. • hmac: The value contains 16 to 64 characters. Letters, digits, and special characters (_-!@\$%) are allowed. It must start with a letter or digit. If not specified, a key is automatically generated. • basic: The value contains 8 to 64 characters. Letters, digits, and special characters (_-!@\$%) are allowed. It must start with a letter or digit. If not specified, a key is automatically generated. • public_key: The value can contain 16 to 2048 characters, including letters, digits, and special characters (_-!@\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated. • aes: The value contains 16 characters, including letters, digits, and special characters (_-!@\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated.
sign_algorithm	String	Signature algorithm. Specify a signature algorithm only when using an AES signature key. By default, no algorithm is used.
update_time	String	Update time.
create_time	String	Creation time.
id	String	Signature key ID.
bind_num	Integer	Number of bound APIs.
ldapi_bind_num	Integer	Number of custom backends bound. Currently, this parameter is not supported.

Status code: 400

Table 4-405 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-406** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-407** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-408** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{  
  "total" : 2,
```

```
"size" : 2,
"signs" : [ {
  "sign_secret" : "sig*****ret",
  "update_time" : "2018-02-07T02:00:27.964766Z",
  "create_time" : "2018-02-06T12:17:36Z",
  "name" : "signature_demo",
  "id" : "0b0e8f456b8742218af75f945307173c",
  "sign_key" : "signkeysignkey",
  "sign_type" : "hmac",
  "bind_num" : 0,
  "ldapi_bind_num" : 0
}, {
  "sign_secret" : "9ce*****16a",
  "update_time" : "2020-07-30T03:56:58Z",
  "create_time" : "2020-07-30T03:56:58Z",
  "name" : "Signature_udlu",
  "id" : "9dc388382fba485aadd19f932303f4c9",
  "sign_key" : "ca50c5b670044c83b5b890a9a68a30d5",
  "sign_type" : "hmac",
  "bind_num" : 0,
  "ldapi_bind_num" : 0
} ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK

Status Code	Description
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.7 Binding/Unbinding Signature Keys

4.7.1 Binding a Signature Key

Function

A signature key takes effect only after being bound to an API.

When requesting the backend service, APIG uses the signature key to cryptographically sign requests. The backend service verifies the signature to identify request sources.

This API is used to bind a signature key to one or more published APIs. You can bind different signature keys to an API in different environments, but can bind only one signature key to the API in each environment.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/sign-bindings

Table 4-409 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-410 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-411 Request body parameters

Parameter	Mandatory	Type	Description
sign_id	Yes	String	Signature key ID.
publish_ids	Yes	Array of strings	API publication record ID.

Response Parameters

Status code: 201

Table 4-412 Response body parameters

Parameter	Type	Description
bindings	Array of SignApiBindingInfo objects	APIs bound to the signature key.

Table 4-413 SignApiBindingInfo

Parameter	Type	Description
publish_id	String	API publication record ID.

Parameter	Type	Description
api_id	String	API ID.
group_name	String	Name of the API group to which the API belongs.
binding_time	String	Binding time.
env_id	String	ID of the environment in which the API has been published.
env_name	String	Name of the environment in which the API has been published.
api_type	Integer	API type.
api_name	String	API name.
id	String	Binding record ID.
api_remark	String	API description.
sign_id	String	Signature key ID.
sign_name	String	Signature key name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
req_method	String	Request method.
tags	Array of strings	Tags bound to the API. The default quota is 10. You can contact technical support to adjust the quota. Minimum: 1 Maximum: 128 Array Length: 0 - 10

Parameter	Type	Description
sign_key	String	Signature key. • hmac: The value contains 8 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter or digit. If not specified, a key is automatically generated. • basic: The value contains 4 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter. If not specified, a key is automatically generated. • public_key: The value contains 8 to 512 characters, including letters, digits, and special characters (_-+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated. • aes: The value contains 16 characters if the aes-128-cfb algorithm is used, or 32 characters if the aes-256-cfb algorithm is used. Letters, digits, and special characters (_-!@\$%+/=) are allowed. It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated.

Parameter	Type	Description
sign_secret	String	Signature secret. • hmac: The value contains 16 to 64 characters. Letters, digits, and special characters (_-!@\$%) are allowed. It must start with a letter or digit. If not specified, a value is automatically generated. • basic: The value contains 8 to 64 characters. Letters, digits, and special characters (_-!@\$%) are allowed. It must start with a letter or digit. If not specified, a value is automatically generated. • public_key: The value contains 15 to 2048 characters, including letters, digits, and special characters (_-!@\$%\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a value is automatically generated. • aes: The value contains 16 characters, including letters, digits, and special characters (_-!@\$%\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a value is automatically generated.

Parameter	Type	Description
sign_type	String	Signature key type: • hmac -basic -public_key -aes To use a basic signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway. To use a public_key signature key, ensure that the public_key feature has been configured for your gateway. For details, see "Appendix" > "Supported Features". If your gateway does not support this feature, contact technical support to enable it. To use an AES signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway.

Status code: 400**Table 4-414** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-415** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-416 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-417** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-418** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Binding a signature key to a published API

```
{
  "sign_id" : "0b0e8f456b8742218af75f945307173c",
  "publish_ids" : [ "40e7162dc6b94bbbbb1a60d2a24b1b0c" ]
}
```

Example Responses

Status code: 201

Created

```
{
  "bindings" : [ {
    "api_id" : "5f918d104dc84480a75166ba99efff21",
    "sign_secret" : "dc0*****2b3",
    "group_name" : "api_group_001",
    "sign_id" : "0b0e8f456b8742218af75f945307173c",
    "sign_key" : "a071a20d460a4f639a636c3d7e3d8163",
    "binding_time" : "2020-08-03T04:00:11.638167852Z",
    "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "env_name" : "RELEASE",
    "sign_name" : "signature_demo",
  } ]
}
```

```
"api_type" : 1,  
"api_name" : "Api_http",  
"id" : "25082bd52f74442bb1d273993d567938",  
"api_remark" : "Web backend API"  
}]  
}
```

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2012",  
  "error_msg" : "Invalid parameter value,parameterName:sign_id. Please refer to the support documentation"  
}
```

Status code: 401

Unauthorized

```
{  
  "error_code" : "APIG.1002",  
  "error_msg" : "Incorrect token or token resolution failed"  
}
```

Status code: 403

Forbidden

```
{  
  "error_code" : "APIG.1005",  
  "error_msg" : "No permissions to request this method"  
}
```

Status code: 404

Not Found

```
{  
  "error_code" : "APIG.3017",  
  "error_msg" : "Signature key 0b0e8f456b8742218af75f945307173c does not exist"  
}
```

Status code: 500

Internal Server Error

```
{  
  "error_code" : "APIG.9999",  
  "error_msg" : "System error"  
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

Status Code	Description
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.7.2 Unbinding a Signature Key

Function

This API is used to unbind a signature key from an API.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/sign-bindings/{sign_bindings_id}

Table 4-419 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
sign_bindings_id	Yes	String	Signature key binding record ID.

Request Parameters

Table 4-420 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-421 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-422 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-423 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-424** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-425** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3018",
}
```

```
{
  "error_msg": "The signature key binding record does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.7.3 Querying Signature Keys Bound to an API

Function

This API is used to query the signature keys that have been bound to a specified API. Only one signature key can be bound to an API in an environment.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/sign-bindings/bindedsigns

Table 4-426 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-427 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
api_id	Yes	String	API ID.
sign_id	No	String	Signature key ID.
sign_name	No	String	Signature key name.
env_id	No	String	Environment ID.

Request Parameters

Table 4-428 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-429 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
bindings	Array of SignApiBindingInfo objects	APIs bound to the signature key.

Table 4-430 SignApiBindingInfo

Parameter	Type	Description
publish_id	String	API publication record ID.
api_id	String	API ID.
group_name	String	Name of the API group to which the API belongs.
binding_time	String	Binding time.
env_id	String	ID of the environment in which the API has been published.
env_name	String	Name of the environment in which the API has been published.
api_type	Integer	API type.
api_name	String	API name.

Parameter	Type	Description
id	String	Binding record ID.
api_remark	String	API description.
sign_id	String	Signature key ID.
sign_name	String	Signature key name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
req_method	String	Request method.
tags	Array of strings	Tags bound to the API. The default quota is 10. You can contact technical support to adjust the quota. Minimum: 1 Maximum: 128 Array Length: 0 - 10
sign_key	String	Signature key. • hmac: The value contains 8 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter or digit. If not specified, a key is automatically generated. • basic: The value contains 4 to 32 characters, including letters, digits, underscores (_), and hyphens (-). It must start with a letter. If not specified, a key is automatically generated. • public_key: The value contains 8 to 512 characters, including letters, digits, and special characters (_-+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated. • aes: The value contains 16 characters if the aes-128-cfb algorithm is used, or 32 characters if the aes-256-cfb algorithm is used. Letters, digits, and special characters (_-!@#\$%+/=) are allowed. It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a key is automatically generated.

Parameter	Type	Description
sign_secret	String	Signature secret. • hmac: The value contains 16 to 64 characters. Letters, digits, and special characters (_-!@\$%) are allowed. It must start with a letter or digit. If not specified, a value is automatically generated. • basic: The value contains 8 to 64 characters. Letters, digits, and special characters (_-!@\$%) are allowed. It must start with a letter or digit. If not specified, a value is automatically generated. • public_key: The value contains 15 to 2048 characters, including letters, digits, and special characters (_-!@\$%\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a value is automatically generated. • aes: The value contains 16 characters, including letters, digits, and special characters (_-!@\$%\$%+/=). It must start with a letter, digit, plus sign (+), or slash (/). If not specified, a value is automatically generated.

Parameter	Type	Description
sign_type	String	Signature key type: • hmac -basic -public_key -aes To use a basic signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway. To use a public_key signature key, ensure that the public_key feature has been configured for your gateway. For details, see "Appendix" > "Supported Features". If your gateway does not support this feature, contact technical support to enable it. To use an AES signature key, ensure that your gateway version supports it. If your gateway does not support this type of signature key, contact technical support to upgrade your gateway.

Status code: 400**Table 4-431** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-432** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-433 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-434 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-435 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "bindings" : [ {
    "api_id" : "5f918d104dc84480a75166ba99efff21",
    "group_name" : "api_group_001",
    "binding_time" : "2020-08-03T04:00:11Z",
    "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "env_name" : "RELEASE",
    "sign_id" : "0b0e8f456b8742218af75f945307173c",
    "sign_name" : "signature_demo",
    "sign_key" : "a071a20d460a4f639a636c3d7e3d8163",
    "sign_secret" : "dc0*****2b3",
    "api_type" : 1,
    "api_name" : "Api_http",
    "id" : "25082bd52f74442bb1d273993d567938",
```

```
{
  "api_remark" : "Web backend API"
}]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:api_name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "API 5f918d104dc84480a75166ba99efff21 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

Status Code	Description
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.7.4 Querying APIs Not Bound with a Signature Key

Function

This API is used to query the APIs to which a signature key has not been bound. Only published APIs will be displayed.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/sign-bindings/unbinded-apis

Table 4-436 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-437 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
sign_id	Yes	String	Signature key ID.
env_id	No	String	Environment ID.
api_id	No	String	API ID.
api_name	No	String	API name.
group_id	No	String	API group ID.
tags	No	String	API tag. Multiple API tags can be specified. The relationship between multiple parameter values is OR. If this parameter is not specified, no filtering tag is specified. If this parameter is set to #no_tags#, APIs without tags are filtered. Minimum: 0 Maximum: 128

Request Parameters

Table 4-438 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-439 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
apis	Array of ApiForSign objects	API list.

Table 4-440 ApiForSign

Parameter	Type	Description
auth_type	String	API authentication mode.
run_env_name	String	Name of the environment in which the API has been published.
group_name	String	Name of the API group to which the API belongs.
publish_id	String	Publication record ID.
group_id	String	ID of the API group to which the API belongs.
name	String	API name.
remark	String	API description.
run_env_id	String	ID of the environment in which the API has been published.
id	String	API ID.
req_uri	String	API request address.
tags	Array of strings	Tags bound to the API. The default quota is 10. You can contact technical support to adjust the quota. Minimum: 1 Maximum: 128 Array Length: 0 - 10
type	Integer	API type.
signature_name	String	Name of the signature key bound to the API.
req_method	String	Request method.

Status code: 400**Table 4-441** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-442** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-443** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-444** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-445** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "apis" : [ {
    "run_env_name" : "RELEASE",
    "group_name" : "api_group_001",
    "remark" : "Mock backend API",
    "publish_id" : "9f27d1dc4f4242a9abf88e563dbfc33d",
    "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
    "name" : "Api_mock",
    "run_env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "id" : "3a955b791bd24b1c9cd94c745f8d1aad",
    "type" : 1,
    "auth_type" : "IAM",
    "req_uri" : "/test/mock"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:api_name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3017",
  "error_msg" : "Signature key 0b0e8f456b8742218af75f945307173c does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.7.5 Querying APIs Bound with a Signature Key

Function

This API is used to query the APIs to which a signature key has been bound.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/sign-bindings/binded-apis

Table 4-446 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-447 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
sign_id	Yes	String	Signature key ID.
env_id	No	String	Environment ID.
api_id	No	String	API ID.
api_name	No	String	API name.
group_id	No	String	API group ID.

Parameter	Mandatory	Type	Description
tags	No	String	API tag. Multiple API tags can be specified. The relationship between multiple parameter values is OR. If this parameter is not specified, no filtering tag is specified. If this parameter is set to #no_tags#, APIs without tags are filtered. Minimum: 0 Maximum: 128

Request Parameters

Table 4-448 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-449 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
bindings	Array of SignApiBindingBase objects	List of signature key binding records.

Table 4-450 SignApiBindingBase

Parameter	Type	Description
publish_id	String	API publication record ID.

Parameter	Type	Description
api_id	String	API ID.
group_name	String	Name of the API group to which the API belongs.
binding_time	String	Binding time.
env_id	String	ID of the environment in which the API has been published.
env_name	String	Name of the environment in which the API has been published.
api_type	Integer	API type.
api_name	String	API name.
id	String	Binding record ID.
api_remark	String	API description.
sign_id	String	Signature key ID.
sign_name	String	Signature key name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
req_method	String	Request method.
tags	Array of strings	Tags bound to the API. The default quota is 10. You can contact technical support to adjust the quota. Minimum: 1 Maximum: 128 Array Length: 0 - 10

Status code: 400**Table 4-451** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-452 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-453** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-454** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-455** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{  
  "total" : 1,
```

```
"size" : 1,
"bindings" : [ {
  "api_id" : "5f918d104dc84480a75166ba99efff21",
  "group_name" : "api_group_001",
  "binding_time" : "2020-08-03T04:00:11Z",
  "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "env_name" : "RELEASE",
  "sign_name" : "signature_demo",
  "api_type" : 1,
  "api_name" : "Api_http",
  "id" : "25082bd52f74442bb1d273993d567938",
  "api_remark" : "Web backend API",
  "publish_id" : "40e7162dc6b94bbbbb1a60d2a24b1b0c"
} ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:api_name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3017",
  "error_msg" : "Signature key 0b0e8f456b8742218af75f945307173c does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.8 Binding/Unbinding Request Throttling Policies

4.8.1 Binding a Request Throttling Policy

Function

The request throttling policy bound to an API will control access of all users to the API.

If the number of API calls within a specified period reaches the limit, subsequent access will be rejected, protecting the backend API from abnormal traffic and ensuring stable service running.

This API is used to bind a request throttling policy to an API that has been published in an environment. You can bind different request throttling policies to an API in different environments, but can bind only one request throttling policy to the API in each environment.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/throttle-bindings

Table 4-456 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-457 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-458 Request body parameters

Parameter	Mandatory	Type	Description
strategy_id	Yes	String	Request throttling policy ID. Minimum: 1 Maximum: 65
publish_ids	Yes	Array of strings	API publication record ID.

Response Parameters

Status code: 201

Table 4-459 Response body parameters

Parameter	Type	Description
throttle_applys	Array of ThrottleApiBinding objects	Request throttling policy binding records.

Table 4-460 ThrottleApiBinding

Parameter	Type	Description
publish_id	String	API publication record ID.
scope	Integer	Scope of the policy. • 1: the API • 2: a user • 3: an app Currently, only "1" is supported.
strategy_id	String	Request throttling policy ID.
apply_time	String	Binding time.
id	String	Binding record ID.

Status code: 401**Table 4-461** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-462** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-463** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-464** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Binding a request throttling policy to an API

```
{
  "publish_ids" : [ "40e7162dc6b94bbbb1a60d2a24b1b0c" ],
  "strategy_id" : "3437448ad06f4e0c91a224183116e965"
}
```

Example Responses**Status code: 201**

Created

```
{
  "throttle_applies" : [ {
    "publish_id" : "40e7162dc6b94bbbb1a60d2a24b1b0c",
    "scope" : 1,
    "strategy_id" : "3437448ad06f4e0c91a224183116e965",
    "apply_time" : "2020-08-03T12:25:52.257613934Z",
    "id" : "3e06ac135e18477e918060d3c59d6f6a"
  } ]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3005",
  "error_msg" : "Request throttling policy 3437448ad06f4e0c91a224183116e965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.8.2 Unbinding a Request Throttling Policy

Function

This API is used to unbind a request throttling policy from an API.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/throttle-bindings/{throttle_binding_id}

Table 4-465 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Parameter	Mandatory	Type	Description
throttle_binding_id	Yes	String	ID of a request throttling policy binding record.

Request Parameters

Table 4-466 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-467 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-468 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-469 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-470** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-471** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3012",
  "error_msg" : "The request throttling policy binding record does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.8.3 Querying APIs Bound with a Request Throttling Policy

Function

This API is used to query the APIs to which a specified request throttling policy has been bound.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/throttle-bindings/binded-apis

Table 4-472 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-473 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
throttle_id	Yes	String	Request throttling policy ID.
env_id	No	String	Environment ID.
group_id	No	String	API group ID.
api_id	No	String	API ID.
api_name	No	String	API name.

Request Parameters

Table 4-474 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-475 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
apis	Array of ApiForThrottle objects	API list.

Table 4-476 ApiForThrottle

Parameter	Type	Description
auth_type	String	API authentication mode.
group_name	String	Name of the API group to which the API belongs.
publish_id	String	API publication record ID.
throttle_apply_id	String	ID of a request throttling policy binding record.
apply_time	String	Binding time.
remark	String	API description.
run_env_id	String	ID of the environment in which the API has been published.
type	Integer	API type.

Parameter	Type	Description
throttle_name	String	Name of the request throttling policy bound to the API.
req_uri	String	Access address of the API.
run_env_name	String	Name of the environment in which the API has been published.
group_id	String	ID of the API group to which the API belongs.
name	String	API name.
id	String	API ID.
req_method	String	Request method.
tags	Array of strings	Tags bound to the API. The default quota is 10. You can contact technical support to adjust the quota. Minimum: 1 Maximum: 128 Array Length: 0 - 10

Status code: 400**Table 4-477** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-478** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-479 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-480** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-481** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total": 1,
  "size": 1,
  "apis": [ {
    "run_env_name": "RELEASE",
    "group_name": "api_group_001",
    "publish_id": "40e7162dc6b94bbbbb1a60d2a24b1b0c",
    "group_id": "c77f5e81d9cb4424bf704ef2b0ac7600",
    "throttle_apply_id": "3e06ac135e18477e918060d3c59d6f6a",
    "name": "Api_http",
    "apply_time": "2020-08-03T12:25:52Z",
    "remark": "Web backend API",
    "run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "id": "5f918d104dc84480a75166ba99efff21",
    "type": 1,
    "throttle_name": "throttle_demo",
```

```
{
  "auth_type": "APP",
  "req_uri": "/test/http"
}]
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2012",
  "error_msg": "Invalid parameter value,parameterName:throttle_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3005",
  "error_msg": "Request throttling policy 3437448ad06f4e0c91a224183116e965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

Status Code	Description
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.8.4 Querying APIs Not Bound with a Request Throttling Policy

Function

This API is used to query the self-developed APIs to which a request throttling policy has not been bound. Only published APIs will be displayed.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/throttle-bindings/unbinded-apis

Table 4-482 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-483 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
throttle_id	Yes	String	Request throttling policy ID.
env_id	No	String	Environment ID.
group_id	No	String	API group ID.
api_id	No	String	API ID.
api_name	No	String	API name.
tags	No	String	API tag. Multiple API tags can be specified. The relationship between multiple parameter values is OR. If this parameter is not specified, no filtering tag is specified. If this parameter is set to #no_tags#, APIs without tags are filtered. Minimum: 0 Maximum: 128

Request Parameters

Table 4-484 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-485 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
apis	Array of ApiForThrottle objects	API list.

Table 4-486 ApiForThrottle

Parameter	Type	Description
auth_type	String	API authentication mode.
group_name	String	Name of the API group to which the API belongs.
publish_id	String	API publication record ID.
throttle_apply_id	String	ID of a request throttling policy binding record.
apply_time	String	Binding time.
remark	String	API description.
run_env_id	String	ID of the environment in which the API has been published.
type	Integer	API type.
throttle_name	String	Name of the request throttling policy bound to the API.
req_uri	String	Access address of the API.
run_env_name	String	Name of the environment in which the API has been published.
group_id	String	ID of the API group to which the API belongs.
name	String	API name.
id	String	API ID.
req_method	String	Request method.

Parameter	Type	Description
tags	Array of strings	Tags bound to the API. The default quota is 10. You can contact technical support to adjust the quota. Minimum: 1 Maximum: 128 Array Length: 0 - 10

Status code: 400**Table 4-487** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-488** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-489** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-490 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-491 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total": 2,
  "size": 2,
  "apis": [ {
    "run_env_name": "RELEASE",
    "group_name": "api_group_001",
    "publish_id": "9f27d1dc4f4242a9abf88e563dbfc33d",
    "group_id": "c77f5e81d9cb4424bf704ef2b0ac7600",
    "name": "Api_mock",
    "remark": "Mock backend API",
    "run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "id": "3a955b791bd24b1c9cd94c745f8d1aad",
    "type": 1,
    "auth_type": "IAM",
    "req_uri": "/test/mock"
  }, {
    "run_env_name": "RELEASE",
    "group_name": "APIGroup_d00511069",
    "publish_id": "0c613568c8644a1b92172156f77a5759",
    "group_id": "d7d0b9a54469424f942e16a6b6026936",
    "name": "API_nevj",
    "run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "id": "9e07bc00a1864ab4aafd4a23d19dd1c2",
    "type": 1,
    "auth_type": "APP",
    "req_uri": "/fdasf"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:throttle_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3005",
  "error_msg" : "Request throttling policy 3437448ad06f4e0c91a224183116e965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.8.5 Querying Request Throttling Policies Bound to an API

Function

This API is used to query the request throttling policies that have been bound to an API. Only one request throttling policy can be bound to an API in an environment.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/throttle-bindings/binded-throttles

Table 4-492 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-493 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
api_id	Yes	String	API ID.
throttle_id	No	String	Request throttling policy ID.
throttle_name	No	String	Request throttling policy name.
env_id	No	String	Environment ID.

Request Parameters

Table 4-494 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-495 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.

Parameter	Type	Description
throttles	Array of ThrottleForApi objects	Request throttling policy list.

Table 4-496 ThrottleForApi

Parameter	Type	Description
app_call_limits	Integer	Maximum number of times the API can be accessed by an app within the same period. The value of this parameter cannot exceed the user call limit. The maximum value is 2,147,483,647. Enter a positive integer.
name	String	Request throttling policy name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
time_unit	String	Time unit for limiting the number of API calls.
remark	String	Description of the request throttling policy, which can contain a maximum of 255 characters.
api_call_limits	Integer	Maximum number of times an API can be accessed within a specified period. The value of this parameter cannot exceed the default limit 200 TPS. You can change the default limit to meet service requirements. The maximum value is 2,147,483,647. Enter a positive integer.
type	Integer	Type of the request throttling policy. • 1: API-based, limiting the maximum number of times a single API bound to the policy can be called within the specified period. • 2: API-shared, limiting the maximum number of times all APIs bound to the policy can be called within the specified period.

Parameter	Type	Description
enable_adaptive_c ontrol	String	Indicates whether to enable dynamic request throttling. • TRUE • FALSE Currently, this parameter is not supported.
user_call_limits	Integer	Maximum number of times the API can be accessed by a user within the same period. The value of this parameter cannot exceed the Max. API Requests. The maximum value is 2,147,483,647. Enter a positive integer.
time_interval	Integer	Period of time for limiting the number of API calls. This parameter applies with each API call limit. The maximum value is 2,147,483,647. Enter a positive integer.
ip_call_limits	Integer	Maximum number of times the API can be accessed by an IP address within the same period. The value of this parameter cannot exceed the API call limit. The maximum value is 2,147,483,647. Enter a positive integer.
id	String	Request throttling policy ID.
bind_num	Integer	Number of APIs to which the request throttling policy has been bound.
is_inclu_special_th rottle	Integer	Indicates whether an excluded request throttling configuration has been created. • 1: yes • 2: no
create_time	String	Creation time.
env_name	String	Environment in which the request throttling policy takes effect.
bind_id	String	Policy binding record ID.
bind_time	String	Time when the policy is bound to the API.

Status code: 400

Table 4-497 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-498** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-499** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-500** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-501** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "throttles" : [ {
    "id" : "3437448ad06f4e0c91a224183116e965",
    "name" : "throttle_demo",
    "api_call_limits" : 800,
    "user_call_limits" : 500,
    "app_call_limits" : 300,
    "ip_call_limits" : 600,
    "time_interval" : 1,
    "time_unit" : "SECOND",
    "create_time" : "2020-07-31T08:44:02Z",
    "remark" : "Total: 800 calls/second; user: 500 calls/second; app: 300 calls/second; IP address: 600 calls/second",
    "is_inclu_special_throttle" : 2,
    "env_name" : "RELEASE",
    "type" : 1,
    "bind_id" : "3e06ac135e18477e918060d3c59d6f6a",
    "bind_time" : "2020-08-03T12:25:52Z",
    "bind_num" : 0,
    "enable_adaptive_control" : "FALSE"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:throttle_name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "API 5f918d104dc84480a75166ba99efff21 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.8.6 Unbinding Request Throttling Policies

Function

This API is used to unbind request throttling policies from APIs.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/throttle-bindings

Table 4-502 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-503 Query Parameters

Parameter	Mandatory	Type	Description
action	Yes	String	The value must be delete.

Request Parameters

Table 4-504 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-505 Request body parameters

Parameter	Mandatory	Type	Description
throttle_bindings	No	Array of strings	IDs of the request throttling policy binding records to be canceled.

Response Parameters

Status code: 200

Table 4-506 Response body parameters

Parameter	Type	Description
success_count	Integer	Number of request throttling policies that have been successfully unbound.
failure	Array of ThrottleBinding-BatchFailure objects	Error message and request throttling policies that fail to be unbound.

Table 4-507 ThrottleBindingBatchFailure

Parameter	Type	Description
bind_id	String	ID of a request throttling policy binding record that fails to be canceled.
error_code	String	Error code.
error_msg	String	Error message.
api_id	String	ID of an API from which unbinding fails.
api_name	String	Name of the API from which unbinding fails.

Status code: 400**Table 4-508** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-509** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-510** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-511** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Unbinding request throttling policies from APIs

```
{
  "throttle_bindings" : [ "6a6a75b425df416cbdc7821da30be8d", "b11e5970f732440dbea647580647d57f" ]
}
```

Example Responses**Status code: 200**

OK

```
{
  "failure" : [ {
    "bind_id" : "b11e5970f732440dbea647580647d57f",
    "error_code" : "APIG.3012",
    "error_msg" : "The request throttling policy binding record does not exist"
  } ],
  "success_count" : 1
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "parameter action should be \\\"delete\\\""
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
}
```

```
{
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.9 Excluded Request Throttling Configuration

4.9.1 Creating an Excluded Request Throttling Configuration

Function

A request throttling policy controls the maximum number of times an API can be accessed within a specified period and the maximum numbers of times the API can be accessed by a tenant or an app within the same period.

If necessary, you can create an excluded request throttling configuration to specify the threshold of API calls for a specific app. For example, if you set the API call threshold for all apps to 500 calls/minute, you can specify the API call threshold of app 1 as 800 calls/minute.

You can add excluded apps or tenants to a request throttling policy.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials

Table 4-512 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
throttle_id	Yes	String	Request throttling policy ID.

Request Parameters

Table 4-513 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-514 Request body parameters

Parameter	Mandatory	Type	Description
call_limits	Yes	Integer	Maximum number of times an excluded object can access an API within the throttling period.
object_id	Yes	String	Excluded app ID or account ID.
object_type	Yes	String	Excluded object type.

Response Parameters

Status code: 201

Table 4-515 Response body parameters

Parameter	Type	Description
id	String	Excluded configuration ID.
call_limits	Integer	Maximum number of times an excluded object can access an API within the throttling period.
apply_time	String	Throttling period.
app_name	String	App name.
app_id	String	App ID.
object_id	String	ID of an object specified in the excluded configuration.
object_type	String	Excluded object type, which can be APP or USER.
object_name	String	Name of an app or a tenant to which the excluded configuration applies.
throttle_id	String	Request throttling policy ID.

Status code: 400

Table 4-516 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-517 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-518** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-519** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-520** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Adding an excluded app to a request throttling policy with threshold 150

```
{
  "call_limits": 150,
  "object_id": "356de8eb7a8742168586e5daf5339965",
  "object_type": "APP"
}
```

Example Responses

Status code: 201

Created

```
{
  "call_limits": 150,
  "app_name": "app_demo",
  "object_name": "app_demo",
  "object_id": "356de8eb7a8742168586e5daf5339965",
  "throttle_id": "3437448ad06f4e0c91a224183116e965",
  "apply_time": "2020-08-04T02:40:56.717710961Z",
}
```

```
{
  "id" : "a3e9ff8db55544ed9db91d8b048770c0",
  "app_id" : "356de8eb7a8742168586e5daf5339965",
  "object_type" : "APP"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2003",
  "error_msg" : "The parameter value is too large,parameterName:call_limits. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3004",
  "error_msg" : "App 356de8eb7a8742168586e5daf5339965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

Status Code	Description
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.9.2 Modifying an Excluded Request Throttling Configuration

Function

This API is used to modify an excluded configuration of a request throttling policy.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials/{strategy_id}

Table 4-521 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
throttle_id	Yes	String	Request throttling policy ID.
strategy_id	Yes	String	Excluded configuration ID.

Request Parameters

Table 4-522 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-523 Request body parameters

Parameter	Mandatory	Type	Description
call_limits	Yes	Long	Maximum number of times an excluded object can access an API within the throttling period.

Response Parameters

Status code: 200

Table 4-524 Response body parameters

Parameter	Type	Description
id	String	Excluded configuration ID.
call_limits	Integer	Maximum number of times an excluded object can access an API within the throttling period.
apply_time	String	Throttling period.
app_name	String	App name.
app_id	String	App ID.
object_id	String	ID of an object specified in the excluded configuration.
object_type	String	Excluded object type, which can be APP or USER.
object_name	String	Name of an app or a tenant to which the excluded configuration applies.
throttle_id	String	Request throttling policy ID.

Status code: 400**Table 4-525** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-526** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-527** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-528** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-529** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Example Requests

Modifying an excluded configuration of a request throttling policy

```
{
  "call_limits" : 200
}
```

Example Responses

Status code: 200

OK

```
{
  "call_limits" : 200,
  "app_name" : "app_demo",
  "object_name" : "app_demo",
  "object_id" : "356de8eb7a8742168586e5daf5339965",
  "throttle_id" : "3437448ad06f4e0c91a224183116e965",
  "apply_time" : "2020-08-04T02:40:56Z",
  "id" : "a3e9ff8db55544ed9db91d8b048770c0",
  "app_id" : "356de8eb7a8742168586e5daf5339965",
  "object_type" : "APP"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2003",
  "error_msg" : "The parameter value is too large,parameterName:call_limits. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3013",
}
```

```
{
  "error_msg": "Excluded request throttling configuration a3e9ff8db55544ed9db91d8b048770c0 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.9.3 Deleting an Excluded Request Throttling Configuration

Function

This API is used to delete an excluded configuration of a request throttling policy.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials/{strategy_id}

Table 4-530 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
throttle_id	Yes	String	Request throttling policy ID.
strategy_id	Yes	String	Excluded configuration ID.

Request Parameters

Table 4-531 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-532 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-533 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-534** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-535** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-536** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2012",  
}
```

```
{
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3013",
  "error_msg" : "Excluded request throttling configuration a3e9ff8db55544ed9db91d8b048770c0 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.9.4 Querying Excluded Request Throttling Configurations

Function

This API is used to query all excluded configurations of a request throttling policy.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials

Table 4-537 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
throttle_id	Yes	String	Request throttling policy ID.

Table 4-538 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20

Parameter	Mandatory	Type	Description
object_type	No	String	Object type, which can be APP or USER.
app_name	No	String	Name of an excluded app.
user	No	String	Name of an excluded user.

Request Parameters

Table 4-539 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-540 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
throttle_specials	Array of ThrottleSpecialInfo objects	Excluded configuration list.

Table 4-541 ThrottleSpecialInfo

Parameter	Type	Description
id	String	Excluded configuration ID.
call_limits	Integer	Maximum number of times an excluded object can access an API within the throttling period.
apply_time	String	Throttling period.

Parameter	Type	Description
app_name	String	App name.
app_id	String	App ID.
object_id	String	ID of an object specified in the excluded configuration.
object_type	String	Excluded object type, which can be APP or USER.
object_name	String	Name of an app or a tenant to which the excluded configuration applies.
throttle_id	String	Request throttling policy ID.

Status code: 400**Table 4-542** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-543** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-544** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-545 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-546** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "throttle_specials" : [ {
    "call_limits" : 200,
    "app_name" : "app_demo",
    "object_name" : "app_demo",
    "object_id" : "356de8eb7a8742168586e5daf5339965",
    "throttle_id" : "3437448ad06f4e0c91a224183116e965",
    "apply_time" : "2020-08-04T02:40:56Z",
    "id" : "a3e9ff8db55544ed9db91d8b048770c0",
    "app_id" : "356de8eb7a8742168586e5daf5339965",
    "object_type" : "APP"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:app_name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
```

```
{
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3005",
  "error_msg": "Request throttling policy 3437448ad06f4e0c91a224183116e965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.10 App Authorization Management

4.10.1 Authorizing Apps

Function

An app cannot access any APIs after being created. To access an API in a specific environment, bind the app to the API in the environment.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/app-auths

Table 4-547 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-548 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-549 Request body parameters

Parameter	Mandatory	Type	Description
env_id	Yes	String	ID of the environment in which the apps will be authorized.

Parameter	Mandatory	Type	Description
app_ids	Yes	Array of strings	App IDs.
api_ids	Yes	Array of strings	API list.

Response Parameters

Status code: 201

Table 4-550 Response body parameters

Parameter	Type	Description
auths	Array of ApiAuthRelations objects	App authorization records.

Table 4-551 ApiAuthRelations

Parameter	Type	Description
api_id	String	API ID.
auth_result	AuthResult object	Authorization result.
auth_time	String	Authorization time.
id	String	Authorization record ID.
app_id	String	App ID.
auth_role	String	Authorizer. • PROVIDER: API provider • CONSUMER: API user
auth_tunnel	String	Authorization channel type. • NORMAL: normal channel • GREEN: green channel The default value is NORMAL. This parameter is not supported currently.
auth_whitelist	Array of strings	Whitelist for the green channel.
auth_blacklist	Array of strings	Blacklist for the green channel.
visit_params	String	Access parameters.

Table 4-552 AuthResult

Parameter	Type	Description
status	String	Authorization result. • SUCCESS • SKIPPED • FAILED
error_msg	String	Error message.
error_code	String	Error code.
api_name	String	Name of the API for which authorization fails.
app_name	String	Name of the app that fails to be authorized.

Status code: 400**Table 4-553** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-554** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-555** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-556** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-557** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Authorizing an app to call an API

```
{
  "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "app_ids" : [ "356de8eb7a8742168586e5daf5339965" ],
  "api_ids" : [ "5f918d104dc84480a75166ba99efff21" ]
}
```

Example Responses

Status code: 201

Created

```
{
  "auths" : [ {
    "api_id" : "5f918d104dc84480a75166ba99efff21",
    "auth_result" : {
      "status" : "SUCCESS"
    },
    "auth_time" : "22020-08-04T04:02:22.482227344Z",
    "id" : "dd29b33ae4394e3b924b582c6b40880b",
    "app_id" : "356de8eb7a8742168586e5daf5339965",
    "auth_role" : "PROVIDER",
    "auth_tunnel" : "NORMAL"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:api_ids. Please refer to the support documentation"
}
```


Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3004",
  "error_msg" : "App 356de8eb7a8742168586e5daf5339965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.10.2 Canceling Authorization

Function

This API is used to cancel the authorization of an app for accessing an API. After this operation, the app can no longer call the API.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/app-auths/{app_auth_id}

Table 4-558 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_auth_id	Yes	String	Authorization record ID.

Request Parameters

Table 4-559 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-560 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-561** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-562** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-563** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-564** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3009",
  "error_msg" : "The app authorization record does not exist,id:dd29b33ae4394e3b924b582c6b40880b"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.10.3 Querying APIs Bound with an App

Function

This API is used to query the APIs to which a specified app has been bound.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/app-auths/binded-apis

Table 4-565 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-566 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
app_id	Yes	String	App ID.
api_id	No	String	API ID.
api_name	No	String	API name.
group_id	No	String	API group ID.
group_name	No	String	API group name.
env_id	No	String	ID of the environment in which the app has been authorized.
tags	No	String	API tag. Multiple API tags can be specified. The relationship between multiple parameter values is OR. If this parameter is not specified, no filtering tag is specified. If this parameter is set to #no_tags#, APIs without tags are filtered. Minimum: 0 Maximum: 128

Request Parameters

Table 4-567 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-568 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
auths	Array of ApiAuthInfo objects	API list.

Table 4-569 ApiAuthInfo

Parameter	Type	Description
id	String	Authorization record ID.
api_id	String	API ID.
api_name	String	API name.
group_name	String	Name of the API group to which the API belongs.
api_type	Integer	API type.
api_remark	String	API description.
env_id	String	ID of the environment in which an app has been authorized to call the API.
auth_role	String	Authorizer.
auth_time	String	Authorization time.
app_name	String	App name.
app_remark	String	App description.
app_type	String	App type. The default value is apig. Other types are not supported currently.
app_creator	String	Creator of the app. • USER: The app is created by a tenant. • MARKET: The app is allocated by KooGallery. This value is not supported currently.

Parameter	Type	Description
publish_id	String	API publication record ID.
group_id	String	ID of the API group to which the API belongs.
auth_tunnel	String	Authorization channel type. • NORMAL: normal channel • GREEN: green channel The default value is NORMAL. This parameter is not supported currently.
auth_whitelist	Array of strings	Whitelist for the green channel.
auth_blacklist	Array of strings	Blacklist for the green channel.
visit_param	String	Access parameters.
roma_app_type	String	ROMA application type. • subscription: subscription application • integration: integration application Currently, this parameter is not supported.
tags	Array of strings	Tags bound to the API. The default quota is 10. You can contact technical support to adjust the quota. Minimum: 1 Maximum: 128 Array Length: 0 - 10
env_name	String	Name of the environment in which the app has been authorized to call the API.
app_id	String	App ID.

Status code: 400**Table 4-570** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-571 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-572** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-573** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-574** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{  
  "total" : 1,
```

```
"size" : 1,
"auths" : [ {
  "api_id" : "5f918d104dc84480a75166ba99efff21",
  "app_name" : "app_demo",
  "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "env_name" : "RELEASE",
  "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "group_name" : "api_group_001",
  "api_type" : 1,
  "api_name" : "Api_http",
  "app_id" : "356de8eb7a8742168586e5daf5339965",
  "auth_time" : "2020-08-04T04:02:22Z",
  "app_creator" : "USER",
  "id" : "dd29b33ae4394e3b924b582c6b40880b",
  "api_remark" : "Web backend Api",
  "auth_role" : "PROVIDER",
  "app_type" : "apig",
  "auth_tunnel" : "NORMAL",
  "publish_id" : "40e7162dc6b94b94b94b94b94b94b94b"
} ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:api_name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3004",
  "error_msg" : "App 356de8eb7a8742168586e5daf5339965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.10.4 Querying APIs Not Bound with an App

Function

This API is used to query the self-developed APIs to which an app has not been bound in a specified environment.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/app-auths/unbinded-apis

Table 4-575 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-576 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
app_id	Yes	String	App ID.
env_id	Yes	String	Environment ID.
group_id	No	String	API group ID.
api_id	No	String	API ID.
api_name	No	String	API name.
tags	No	String	API tag. Multiple API tags can be specified. The relationship between multiple parameter values is OR. If this parameter is not specified, no filtering tag is specified. If this parameter is set to #no_tags#, APIs without tags are filtered. Minimum: 0 Maximum: 128

Request Parameters

Table 4-577 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-578 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
apis	Array of ApiOutline objects	API list.

Table 4-579 ApiOutline

Parameter	Type	Description
auth_type	String	API authentication mode.
run_env_name	String	Name of the environment in which the API has been published.
group_name	String	Name of the API group to which the API belongs.
publish_id	String	Publication record ID.
group_id	String	ID of the API group to which the API belongs.
name	String	API name.
remark	String	API description.
run_env_id	String	ID of the environment in which the API has been published.

Parameter	Type	Description
id	String	API ID.
req_uri	String	API request address.
tags	Array of strings	Tags bound to the API. The default quota is 10. You can contact technical support to adjust the quota. Minimum: 1 Maximum: 128 Array Length: 0 - 10

Status code: 400**Table 4-580** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-581** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-582** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-583 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-584 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total": 2,
  "size": 2,
  "apis": [ {
    "auth_type": "APP",
    "run_env_name": "",
    "group_name": "api_group_001",
    "publish_id": "",
    "group_id": "c77f5e81d9cb4424bf704ef2b0ac7600",
    "name": "Api_function",
    "remark": "FunctionGraph backend API",
    "run_env_id": "",
    "id": "abd9c4b2ff974888b0ba79be7e6b2763",
    "req_uri": "/test/function"
  }, {
    "auth_type": "APP",
    "run_env_name": "RELEASE",
    "group_name": "APIGroup_d3da",
    "publish_id": "ca2631e233a74a758744ae1e19cc5ad7",
    "group_id": "6acd94abe58747ee8a73b10c70817bac",
    "name": "API_test",
    "remark": "FunctionGraph backend API",
    "run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "id": "11cbec3a7a8345ca981b86d161bc436e",
    "req_uri": "/appcode"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:api_name. Please refer to the support
documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3004",
  "error_msg" : "App 356de8eb7a8742168586e5daf5339965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.10.5 Querying Apps Bound to an API

Function

This API is used to query the apps that have been bound to a specified API.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/app-auths/binded-apps

Table 4-585 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-586 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
api_id	No	String	API ID.

Parameter	Mandatory	Type	Description
app_name	No	String	App name.
app_id	No	String	App ID.
env_id	No	String	Environment ID.

Request Parameters

Table 4-587 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-588 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
auths	Array of ApiAuthInfo objects	API list.

Table 4-589 ApiAuthInfo

Parameter	Type	Description
id	String	Authorization record ID.
api_id	String	API ID.
api_name	String	API name.
group_name	String	Name of the API group to which the API belongs.

Parameter	Type	Description
api_type	Integer	API type.
api_remark	String	API description.
env_id	String	ID of the environment in which an app has been authorized to call the API.
auth_role	String	Authorizer.
auth_time	String	Authorization time.
app_name	String	App name.
app_remark	String	App description.
app_type	String	App type. The default value is apig. Other types are not supported currently.
app_creator	String	Creator of the app. • USER: The app is created by a tenant. • MARKET: The app is allocated by KooGallery. This value is not supported currently.
publish_id	String	API publication record ID.
group_id	String	ID of the API group to which the API belongs.
auth_tunnel	String	Authorization channel type. • NORMAL: normal channel • GREEN: green channel The default value is NORMAL. This parameter is not supported currently.
auth_whitelist	Array of strings	Whitelist for the green channel.
auth_blacklist	Array of strings	Blacklist for the green channel.
visit_param	String	Access parameters.
roma_app_type	String	ROMA application type. • subscription: subscription application • integration: integration application Currently, this parameter is not supported.

Parameter	Type	Description
tags	Array of strings	Tags bound to the API. The default quota is 10. You can contact technical support to adjust the quota. Minimum: 1 Maximum: 128 Array Length: 0 - 10
env_name	String	Name of the environment in which the app has been authorized to call the API.
app_id	String	App ID.

Status code: 400**Table 4-590** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-591** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-592** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-593 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-594 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total": 1,
  "size": 1,
  "auths": [ {
    "api_id": "5f918d104dc84480a75166ba99efff21",
    "app_name": "app_demo",
    "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "env_name": "RELEASE",
    "group_id": "c77f5e81d9cb4424bf704ef2b0ac7600",
    "group_name": "api_group_001",
    "api_type": 1,
    "api_name": "Api_http",
    "app_id": "356de8eb7a8742168586e5daf5339965",
    "auth_time": "2020-08-04T04:02:22Z",
    "app_creator": "USER",
    "id": "dd29b33ae4394e3b924b582c6b40880b",
    "api_remark": "Web backend API",
    "auth_role": "PROVIDER",
    "app_type": "apig",
    "auth_tunnel": "NORMAL"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2012",
  "error_msg": "Invalid parameter value,parameterName:app_name. Please refer to the support
```

```
documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "API 5f918d104dc84480a75166ba99efff21 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.11 Resource Query

4.11.1 Querying API Quantities

Function

This API is used to query the number of APIs that have been published in the RELEASE environment and the number of APIs that have not been published in this environment.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/resources/outline/apis

Table 4-595 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-596 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-597 Response body parameters

Parameter	Type	Description
instance_num	Integer	Total number of APIs.
nums_on_release	Integer	Number of APIs that have been published in the RELEASE environment.
nums_off_release	Integer	Number of APIs that have not been published in the RELEASE environment.

Status code: 400**Table 4-598** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-599** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-600** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-601 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-602 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "instance_num" : 27,
  "nums_on_release" : 11,
  "nums_off_release" : 6
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
}
```

```
{
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Bad Request

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Bad Request
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.11.2 Querying API Group Quantities

Function

This API is used to query the number of API groups that have been listed on KooGallery and the number of API groups that have not been listed.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/resources/outline/groups

Table 4-603 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-604 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-605 Response body parameters

Parameter	Type	Description
offsell_nums	Integer	Number of API groups that have not been listed on KooGallery. Currently, this parameter is not supported.
onsell_nums	Integer	Number of API groups that have been listed on KooGallery.

Status code: 400

Table 4-606 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 401**Table 4-607** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-608** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-609** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-610** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "offsell_nums" : 0,
  "onsell_nums" : 23
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.11.3 Querying App Quantities

Function

This API is used to query the number of apps that have been authorized to access APIs and the number of apps that have not been authorized to access any APIs.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/resources/outline/apps

Table 4-611 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-612 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-613** Response body parameters

Parameter	Type	Description
authed_nums	Integer	Number of apps that have been authorized to access APIs.
unauthed_nums	Integer	Number of apps that have not been authorized to access APIs.

Status code: 400**Table 4-614** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-615** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-616 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-617** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-618** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "authenticated_nums" : 7,
  "unauthenticated_nums" : 5
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Bad Request

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Bad Request
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.12 Domain Name Management

4.12.1 Binding a Domain Name

Function

A user-defined domain name takes effect only after an A record set has been added. For details, see section "Adding an A Record Set" in the Domain Name Service User Guide.

An API group can be bound with a maximum of five domain names. After you bind a domain name to an API group, APIs in the group can be called using the domain name.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains

Table 4-619 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.

Request Parameters

Table 4-620 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-621 Request body parameters

Parameter	Mandatory	Type	Description
min_ssl_version	No	String	Minimum SSL version. TLS 1.1 and TLS 1.2 are supported. Default: TLSv1.1
is_http_redirect_to_https	No	Boolean	Whether to enable HTTP redirection to HTTPS. The value false means disable and true means enable. The default value is false. Default: false
ingress_http_port	No	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151

Parameter	Mandatory	Type	Description
ingress_https_port	No	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
url_domain	Yes	String	Custom domain name. The value contains 0 to 255 characters and must comply with the domain name specifications (matching the regular expression '^([a-zA-Z0-9]([a-zA-Z0-9-]{0,61}[a-zA-Z0-9])?\.){1,7}[a-zA-Z]{2,64}\.?\$' or '^([\.[a-zA-Z0-9]([a-zA-Z0-9-]{0,61}[a-zA-Z0-9])?)\{1,6\}\.[a-zA-Z]{2,64}\.?\$'). Minimum: 0 Maximum: 255

Response Parameters

Status code: 201

Table 4-622 Response body parameters

Parameter	Type	Description
url_domain	String	Custom domain name.
id	String	Domain ID.
status	Integer	CNAME resolution status. • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
min_ssl_version	String	Minimum SSL version supported.
is_http_redirect_to_https	Boolean	Whether to enable HTTP redirection to HTTPS. The value false means disable and true means enable. The default value is false. Default: false
verified_client_certificate_enabled	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false
ingress_http_port	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151

Parameter	Type	Description
ingress_https_port	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151

Status code: 400**Table 4-623** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-624** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-625 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-626** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-627** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Binding a domain name to an API group

```
{
  "url_domain": "www.company.com"
}
```

Example Responses

Status code: 201

Created

```
{
  "url_domain": "www.company.com",
  "id": "c5e0d5ba62a34d26ad5c709ae22c1a17",
  "status": 3,
  "min_ssl_version": "TLSv1.1",
  "is_http_redirect_to_https": false,
  "verified_client_certificate_enabled": false
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2024",
  "error_msg" : "Invalid URL domain name"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3001",
  "error_msg" : "API group c77f5e81d9cb4424bf704ef2b0ac7600 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.12.2 Adding a Certificate to a Domain Name

Function

When you create an API to be accessed through HTTPS, you must add an SSL certificate to the independent domain name that has been bound to the group the API belongs to.

For gateways with custom inbound ports, the same domain name is bound to a certificate at the same time. Enabling or disabling client verification takes effect for different ports of the same domain name.

This API is used to add a certificate to a specific domain name.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate

Table 4-628 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.
domain_id	Yes	String	Domain ID.

Request Parameters

Table 4-629 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-630 Request body parameters

Parameter	Mandatory	Type	Description
cert_content	Yes	String	Certificate content.
name	Yes	String	Certificate name. It can contain 4 to 50 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
private_key	Yes	String	Private key.

Response Parameters

Status code: 201

Table 4-631 Response body parameters

Parameter	Type	Description
url_domain	String	Custom domain name.
id	String	Domain ID.
status	Integer	CNAME resolution status. • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
min_ssl_version	String	Minimum SSL version supported.
is_http_redirect_to_https	Boolean	Whether to enable HTTP redirection to HTTPS. The value false means disable and true means enable. The default value is false. Default: false
verified_client_certificate_enabled	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false

Parameter	Type	Description
ingress_http_port	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ingress_https_port	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ssl_name	String	Certificate name.
ssl_id	String	Certificate ID.
ssl_infos	Array of SslInfo objects	SSL certificate list.

Table 4-632 SslInfo

Parameter	Type	Description
ssl_id	String	SSL certificate ID.
ssl_name	String	SSL certificate name.
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2
type	String	Certificate scope: • instance • global Default: global

Status code: 400**Table 4-633** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-634** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-635** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-636** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-637** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Binding a certificate to a domain name

```
{
  "name" : "cert_demo",
  "private_key" : ""-----BEGIN PRIVATE KEY-----THIS IS YOUR PRIVATE KEY-----END PRIVATE KEY-----\\n",
  "cert_content" : ""-----BEGIN CERTIFICATE-----THIS IS YOUR CERT CONTENT-----END CERTIFICATE-----\\n"
}
```

Example Responses

Status code: 201

Created

```
{
  "ssl_name" : "cert_demo",
  "url_domain" : "www.example.com",
  "ssl_id" : "a27be832f2e9441c8127fe48e3b5ac67",
  "id" : "f6bb84ccf1c34035878aa51b7253b21c",
  "status" : 3
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
}
```

```
{
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3020",
  "error_msg": "The URL domain does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.12.3 Modifying a Domain Name

Function

This API is used to modify the configuration of a domain name bound to an API group. For gateways with custom inbound ports, enabling or disabling client verification takes effect for different ports of the same domain name.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}

Table 4-638 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.
domain_id	Yes	String	Domain ID.

Request Parameters

Table 4-639 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-640 Request body parameters

Parameter	Mandatory	Type	Description
min_ssl_version	Yes	String	Minimum SSL version. TLS 1.1 and TLS 1.2 are supported. Default: TLSv1.1

Parameter	Mandatory	Type	Description
is_http_redirect_to_https	No	Boolean	Whether to enable HTTP redirection to HTTPS. The value false means disable and true means enable. The default value is false. Default: false
verified_client_certificate_enabled	No	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false
ingress_http_port	No	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151

Parameter	Mandatory	Type	Description
ingress_https_port	No	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151

Response Parameters

Status code: 201

Table 4-641 Response body parameters

Parameter	Type	Description
url_domain	String	Custom domain name.
id	String	Domain ID.
status	Integer	CNAME resolution status. • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
min_ssl_version	String	Minimum SSL version supported.

Parameter	Type	Description
is_http_redirect_to_https	Boolean	Whether to enable HTTP redirection to HTTPS. The value false means disable and true means enable. The default value is false. Default: false
verified_client_certificate_enabled	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false
ingress_http_port	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151

Parameter	Type	Description
ingress_https_port	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151

Status code: 400**Table 4-642** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-643** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-644 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-645** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-646** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Modifying a domain name

```
{
  "min_ssl_version" : "TLSv1.2"
}
```

Example Responses

Status code: 201

Created

```
{
  "id" : "0a515af69f4e4dcca84fbf85f68c0e27",
  "url_domain" : "www.example.com",
  "status" : 3,
  "min_ssl_version" : "TLSv1.2",
  "is_http_redirect_to_https" : false,
  "verified_client_certificate_enabled" : false
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.3474",
  "error_msg" : "The API group ID in the URL does not match the API group to which the URL domain has been bound"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3020",
  "error_msg" : "The URL domain does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.12.4 Unbinding a Domain Name

Function

This API is used to unbind a custom domain name from an API group.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}

Table 4-647 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.
domain_id	Yes	String	Domain ID.

Request Parameters

Table 4-648 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-649 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-650** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-651** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-652** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-653** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.3474",
  "error_msg" : "The API group ID in the URL does not match the API group to which the URL domain has been bound"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3020",
  "error_msg" : "The URL domain does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.12.5 Setting Accessibility of a Debugging Domain Name

Function

This API is used to disable or enable the debugging domain name bound to an API group.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/sl-domain-access-settings

Table 4-654 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.

Request Parameters

Table 4-655 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-656 Request body parameters

Parameter	Mandatory	Type	Description
sl_domain_access_enabled	Yes	Boolean	Specifies whether the debugging domain name is accessible. Options: true and false. Default: true

Response Parameters

Status code: 204

OK

Status code: 400

Table 4-657 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-658 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-659** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-660** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-661** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Setting accessibility of a debugging domain name

```
{
  "sl_domain_access_enabled" : true
}
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:sl_domain_access_enabled"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3020",
  "error_msg" : "The URL domain does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.12.6 Deleting the Certificate Bound to a Domain Name

Function

This API is used to delete a certificate that is no longer needed or has expired. For gateways with custom inbound ports, the same domain name will be unbound from the certificate at the same time.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate/{certificate_id}

Table 4-662 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.
domain_id	Yes	String	Domain ID.
certificate_id	Yes	String	Certificate ID.

Request Parameters

Table 4-663 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-664 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-665** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-666** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-667** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-668** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:domain_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3020",
  "error_msg" : "The URL domain does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.12.7 Querying Details of the Certificate Bound to a Domain Name

Function

This API is used to query the details of the certificate bound to a domain name.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate/{certificate_id}

Table 4-669 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.
domain_id	Yes	String	Domain ID.
certificate_id	Yes	String	Certificate ID.

Request Parameters

Table 4-670 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-671** Response body parameters

Parameter	Type	Description
id	String	Certificate ID.
name	String	Certificate name.
type	String	Certificate type. Options: • global: Global certificate. • instance: Gateway certificate.
instance_id	String	Gateway ID. • If type is set to global, the default value is common. • If type is set to instance, a gateway ID is displayed.
project_id	String	Project ID.
create_time	String	Creation time.
update_time	String	Update time.
common_name	String	Certificate domain name.
san	Array of strings	Subject alternative names.
version	Integer	Certificate version.
organization	Array of strings	Company or organization.
organizational_unit	Array of strings	Department.
locality	Array of strings	City.
state	Array of strings	State or province.

Parameter	Type	Description
country	Array of strings	Country or region.
not_before	String	Start time of the certificate validity period.
not_after	String	End time of the certificate validity period.
serial_number	String	Serial No.
issuer	Array of strings	Certificate issuer.
signature_algorithm	String	Signature algorithm.

Status code: 400**Table 4-672** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-673** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-674** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-675 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-676** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "serial_number" : "219450666855693268010130472645821723203",
  "version" : 3,
  "san" : [ "www.company.com" ],
  "not_before" : "2019-06-01T00:00:00Z",
  "issuer" : [ "mkcert development CA" ],
  "not_after" : "2030-08-04T07:41:19Z",
  "organization" : [ "mkcert development certificate" ],
  "signature_algorithm" : "SHA256-RSA",
  "organizational_unit" : [ "XXX\\\\\\DESKTOP-L2TFOFH" ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:domain_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3020",
  "error_msg" : "The URL domain does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.13 Access Control Policy Management

4.13.1 Creating an Access Control Policy

Function

This API is used to create an access control policy to allow or deny API access from certain IP addresses or tenants. The `acl_value` value of a domain is a tenant name rather than a domain name (such as `www.exampleDomain.com`).

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/acls

Table 4-677 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-678 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-679 Request body parameters

Parameter	Mandatory	Type	Description
acl_name	Yes	String	Access control policy name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
acl_type	Yes	String	Type. - PERMIT (whitelist) - DENY (blacklist)

Parameter	Mandatory	Type	Description
acl_value	Yes	String	One or more objects from which the access will be controlled. Separate multiple objects with commas. • If entity_type is set to IP, enter up to 100 IP addresses. • If entity_type is set to DOMAIN, enter account names. Each account name can contain up to 64 ASCII characters except commas (,). Do not use only digits. The total length cannot exceed 1024 characters. • If entity_type is set to DOMAIN_ID, enter account IDs. For details about how to obtain an account ID, see "Appendix" > "Obtaining an Account Name and Account ID" in this document.
entity_type	Yes	String	Object type. • IP: IP address. • DOMAIN: Account name. • DOMAIN_ID: Account ID.

Response Parameters

Status code: 201

Table 4-680 Response body parameters

Parameter	Type	Description
acl_name	String	Name.
acl_type	String	Type. • PERMIT (whitelist) • DENY (blacklist)
acl_value	String	Access control objects.

Parameter	Type	Description
entity_type	String	Object type. • IP • DOMAIN • DOMAIN_ID
id	String	ID.
update_time	String	Update time.

Status code: 400**Table 4-681** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-682** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-683** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-684 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-685** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Creating an access control policy to allow access from specified IP addresses

```
{
  "acl_name" : "acl_demo",
  "acl_type" : "PERMIT",
  "acl_value" : "192.168.1.5,192.168.10.1",
  "entity_type" : "IP"
}
```

Example Responses

Status code: 201

Created

```
{
  "id" : "7eb619ecf2a24943b099833cd24a01ba",
  "acl_name" : "acl_demo",
  "entity_type" : "IP",
  "acl_type" : "PERMIT",
  "acl_value" : "192.168.1.5,192.168.10.1",
  "update_time" : "2020-08-04T08:42:43.461276217Z"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:acl_type. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
}
```



```
{
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3030",
  "error_msg": "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.13.2 Modifying an Access Control Policy

Function

This API is used to modify an access control policy. Only attributes `acl_name`, `acl_type`, and `acl_value` can be modified.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/acls/{acl_id}

Table 4-686 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
acl_id	Yes	String	Access control policy ID.

Request Parameters

Table 4-687 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-688 Request body parameters

Parameter	Mandatory	Type	Description
acl_name	Yes	String	Access control policy name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
acl_type	Yes	String	Type. • PERMIT (whitelist) • DENY (blacklist)

Parameter	Mandatory	Type	Description
acl_value	Yes	String	One or more objects from which the access will be controlled. Separate multiple objects with commas. • If entity_type is set to IP, enter up to 100 IP addresses. • If entity_type is set to DOMAIN, enter account names. Each account name can contain up to 64 ASCII characters except commas (,). Do not use only digits. The total length cannot exceed 1024 characters. • If entity_type is set to DOMAIN_ID, enter account IDs. For details about how to obtain an account ID, see "Appendix" > "Obtaining an Account Name and Account ID" in this document.
entity_type	Yes	String	Object type. • IP: IP address. • DOMAIN: Account name. • DOMAIN_ID: Account ID.

Response Parameters

Status code: 200

Table 4-689 Response body parameters

Parameter	Type	Description
acl_name	String	Name.
acl_type	String	Type. • PERMIT (whitelist) • DENY (blacklist)
acl_value	String	Access control objects.

Parameter	Type	Description
entity_type	String	Object type. • IP • DOMAIN • DOMAIN_ID
id	String	ID.
update_time	String	Update time.

Status code: 400**Table 4-690** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-691** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-692** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-693 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-694** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Updating an access control policy to allow access from specified IP addresses

```
{
  "acl_name" : "acl_demo",
  "entity_type" : "IP",
  "acl_type" : "PERMIT",
  "acl_value" : "192.168.1.5,192.168.10.1"
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "7eb619ecf2a24943b099833cd24a01ba",
  "acl_name" : "acl_demo",
  "entity_type" : "IP",
  "acl_type" : "PERMIT",
  "acl_value" : "192.168.1.5,192.168.10.1",
  "update_time" : "2020-08-04T08:54:55.975856802Z"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:acl_type. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
}
```

```
{
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3006",
  "error_msg": "Access control policy 7eb619ecf2a24943b099833cd24a01ba does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.13.3 Deleting an Access Control Policy

Function

This API is used to delete an access control policy. Access control policies bound to APIs cannot be deleted.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/acls/{acl_id}

Table 4-695 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
acl_id	Yes	String	Access control policy ID.

Request Parameters

Table 4-696 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-697 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-698** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-699** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-700** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-701** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 400**

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3006",
  "error_msg" : "Access control policy 7eb619ecf2a24943b099833cd24a01ba does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.13.4 Deleting Multiple Access Control Policies

Function

This API is used to delete multiple access control policies.

Access control policies bound to APIs cannot be deleted.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/acls

Table 4-702 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-703 Query Parameters

Parameter	Mandatory	Type	Description
action	Yes	String	The value must be delete.

Request Parameters

Table 4-704 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-705 Request body parameters

Parameter	Mandatory	Type	Description
acls	No	Array of strings	IDs of the access control policies to be deleted.

Response Parameters

Status code: 200

Table 4-706 Response body parameters

Parameter	Type	Description
success_count	Integer	Number of access control policies that have been successfully deleted.
failure	Array of AclBatchResultFailureResp objects	Error message and access control policies that fail to be deleted.

Table 4-707 AclBatchResultFailureResp

Parameter	Type	Description
acl_id	String	ID of an access control policy that fails to be deleted.
acl_name	String	Name of the access control policy.
error_code	String	Error code.
error_msg	String	Error message.

Status code: 400

Table 4-708 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-709 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-710** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-711** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-712** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Deleting multiple access control policies

```
{
  "acls" : [ "7eb619ecf2a24943b099833cd24a01ba", "3a68d39f115d4c128fccd6f624ea6109" ]
}
```

Example Responses

Status code: 200

OK

```
{
  "failure": [ {
    "acl_id": "7eb619ecf2a24943b099833cd24a01ba",
    "acl_name": "acl_demo",
    "error_code": "APIG.3447",
    "error_msg": "The access control policy has been bound to APIs"
  } ],
  "success_count": 1
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2011",
  "error_msg": "Invalid parameter value: parameter action should be \\\"delete\\\""
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3030",
  "error_msg": "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request

Status Code	Description
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.13.5 Querying Details of an Access Control Policy

Function

This API is used to query the details of an access control policy.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/acls/{acl_id}

Table 4-713 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
acl_id	Yes	String	Access control policy ID.

Request Parameters

Table 4-714 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-715** Response body parameters

Parameter	Type	Description
acl_name	String	Name.
acl_type	String	Type. • PERMIT (whitelist) • DENY (blacklist)
acl_value	String	Access control objects.
entity_type	String	Object type. • IP • DOMAIN • DOMAIN_ID
id	String	ID.
update_time	String	Update time.

Status code: 400**Table 4-716** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-717 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-718** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-719** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-720** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{  
  "id" : "7eb619ecf2a24943b099833cd24a01ba",  
}
```



```
"acl_name" : "acl_demo",  
"entity_type" : "IP",  
"acl_type" : "PERMIT",  
"acl_value" : "192.168.1.5,192.168.10.1",  
"update_time" : "2020-08-04T08:42:43Z"  
}
```

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2011",  
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"  
}
```

Status code: 401

Unauthorized

```
{  
  "error_code" : "APIG.1002",  
  "error_msg" : "Incorrect token or token resolution failed"  
}
```

Status code: 403

Forbidden

```
{  
  "error_code" : "APIG.1005",  
  "error_msg" : "No permissions to request this method"  
}
```

Status code: 404

Not Found

```
{  
  "error_code" : "APIG.3006",  
  "error_msg" : "Access control policy 7eb619ecf2a24943b099833cd24a01ba does not exist"  
}
```

Status code: 500

Internal Server Error

```
{  
  "error_code" : "APIG.9999",  
  "error_msg" : "System error"  
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

Status Code	Description
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.13.6 Querying Access Control Policies

Function

This API is used to query all the access control policies.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/acls

Table 4-721 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-722 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
id	No	String	Access control policy ID.
name	No	String	Access control policy name.
acl_type	No	String	Type. • PERMIT (whitelist) • DENY (blacklist)
entity_type	No	String	Object types. • IP • DOMAIN
precise_search	No	String	Parameter name (name) for exact matching.

Request Parameters

Table 4-723 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-724 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
acls	Array of ApiAclInfoWithBindNum objects	Access control policy list.

Table 4-725 ApiAclInfoWithBindNum

Parameter	Type	Description
acl_name	String	Access control policy name.
acl_type	String	Type. - PERMIT (whitelist) - DENY (blacklist)
acl_value	String	Access control objects.
bind_num	Integer	Number of APIs.
entity_type	String	Object type. - IP - DOMAIN - DOMAIN_ID
id	String	Access control policy ID.
update_time	String	Update time.

Status code: 400**Table 4-726** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-727 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-728** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-729** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-730** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{  
  "total" : 1,
```

```
"size" : 1,
"acls" : [ {
  "bind_num" : 0,
  "id" : "7eb619ecf2a24943b099833cd24a01ba",
  "acl_name" : "acl_demo",
  "entity_type" : "IP",
  "acl_type" : "PERMIT",
  "acl_value" : "192.168.1.5,192.168.10.1",
  "update_time" : "2020-08-04T08:42:43Z"
} ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request

Status Code	Description
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.14 Binding/Unbinding Access Control Policies

4.14.1 Binding an Access Control Policy to an API

Function

This API is used to bind an access control policy to a specified API.

You can bind different access control policies to an API in different environments, but you can bind only one access control policy to the API in each environment.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/acl-bindings

Table 4-731 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-732 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-733 Request body parameters

Parameter	Mandatory	Type	Description
acl_id	No	String	Access control policy ID.
publish_ids	No	Array of strings	API publication record ID.

Response Parameters

Status code: 201

Table 4-734 Response body parameters

Parameter	Type	Description
acl_bindings	Array of AclApiBindingInfo objects	Access control policy binding records.

Table 4-735 AclApiBindingInfo

Parameter	Type	Description
id	String	Binding record ID.
api_id	String	API ID.
env_id	String	Environment ID.
acl_id	String	Access control policy ID.
create_time	String	Binding time.

Status code: 400

Table 4-736 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-737** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-738** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-739** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-740** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Binding an access control policy to an API

```
{
  "acl_id" : "7eb619ecf2a24943b099833cd24a01ba",
  "publish_ids" : [ "40e7162dc6b94bbbb1a60d2a24b1b0c" ]
}
```

Example Responses

Status code: 201

Created

```
{
  "acl_bindings" : [ {
    "id" : "332c5db1458a477b89b2ea741fec94a3",
    "api_id" : "5f918d104dc84480a75166ba99efff21",
    "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "acl_id" : "7eb619ecf2a24943b099833cd24a01ba",
    "create_time" : "2020-08-04T08:58:03.001228747Z"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:acl_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3006",
  "error_msg" : "Access control policy 7eb619ecf2a24943b099833cd24a01ba does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
}
```

```
"error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.14.2 Unbinding an Access Control Policy

Function

This API is used to unbind an access control policy from an API.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/acl-bindings/{acl_bindings_id}

Table 4-741 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Parameter	Mandatory	Type	Description
acl_bindings_id	Yes	String	Binding record ID.

Request Parameters

Table 4-742 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-743 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-744 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-745 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-746** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-747** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3010",
  "error_msg" : "The access control policy binding record does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.14.3 Unbinding Access Control Policies

Function

This API is used to unbind multiple access control policies from APIs.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/acl-bindings

Table 4-748 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-749 Query Parameters

Parameter	Mandatory	Type	Description
action	Yes	String	The value must be delete.

Request Parameters

Table 4-750 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-751 Request body parameters

Parameter	Mandatory	Type	Description
acl_bindings	No	Array of strings	IDs of the access control policy binding records to be canceled.

Response Parameters

Status code: 200

Table 4-752 Response body parameters

Parameter	Type	Description
success_count	Integer	Number of access control policies that have been successfully unbound.
failure	Array of AclBindingBatch-Failure objects	Error message and access control policies that fail to be unbound.

Table 4-753 AclBindingBatchFailure

Parameter	Type	Description
bind_id	String	ID of an access control policy binding record that fails to be canceled.
error_code	String	Error code.
error_msg	String	Error message.
api_id	String	ID of an API from which unbinding fails.
api_name	String	Name of the API from which unbinding fails.

Status code: 400**Table 4-754** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-755** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-756 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-757** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-758** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Unbinding multiple access control policies from APIs

```
{
  "acl_bindings" : [ "332c5db1458a477b89b2ea741fec94a3" ]
}
```

Example Responses

Status code: 200

OK

```
{
  "failure" : [ {
    "bind_id" : "3a68d39f115d4c128fccd6f624ea6109",
    "error_code" : "APIG.3010",
    "error_msg" : "The access control policy binding record does not exist"
  } ],
  "success_count" : 1
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value: parameter action should be \\\\\"delete\\\\\""
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.14.4 Querying APIs Bound with an Access Control Policy

Function

This API is used to query the APIs to which an access control policy has been bound.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/acl-bindings/binded-apis

Table 4-759 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-760 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
acl_id	Yes	String	Access control policy ID.

Parameter	Mandatory	Type	Description
api_id	No	String	API ID.
api_name	No	String	API name.
env_id	No	String	Environment ID.
group_id	No	String	API group ID.
tags	No	String	API tag. Multiple API tags can be specified. The relationship between multiple parameter values is OR. If this parameter is not specified, no filtering tag is specified. If this parameter is set to #no_tags#, APIs without tags are filtered. Minimum: 0 Maximum: 128

Request Parameters

Table 4-761 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-762 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
apis	Array of AclBindApiInfo objects	API list.

Table 4-763 AclBindApiInfo

Parameter	Type	Description
api_id	String	API ID.
api_name	String	API name.
api_type	Long	API type.
api_remark	String	API description.
env_id	String	ID of the environment in which the policy takes effect.
env_name	String	Name of the environment in which the policy takes effect.
bind_id	String	Binding record ID.
group_name	String	API group name.
bind_time	String	Binding time.
publish_id	String	API publication record ID.
req_method	String	Request method.
tags	Array of strings	Tags bound to the API. The default quota is 10. You can contact technical support to adjust the quota. Minimum: 1 Maximum: 128 Array Length: 0 - 10

Status code: 400**Table 4-764** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-765** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 403**Table 4-766** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-767** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-768** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{  
  "total" : 1,  
  "size" : 1,  
  "apis" : [ {
```

```
{
  "api_id" : "5f918d104dc84480a75166ba99efff21",
  "api_name" : "Api_http",
  "group_name" : "api_group_001",
  "api_type" : 1,
  "api_remark" : "Web backend API",
  "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "env_name" : "RELEASE",
  "bind_id" : "332c5db1458a477b89b2ea741fec94a3",
  "bind_time" : "2020-08-04T08:58:03Z",
  "publish_id" : "40e7162dc6b94b1a60d2a24b1b0c"
}]
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:api_name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3006",
  "error_msg" : "Access control policy 7eb619ecf2a24943b099833cd24a01ba does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK

Status Code	Description
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.14.5 Querying APIs Not Bound with an Access Control Policy

Function

This API is used to query the published APIs to which an access control policy has not been bound.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/acl-bindings/unbinded-apis

Table 4-769 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-770 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
acl_id	Yes	String	Access control policy ID.
api_id	No	String	API ID.
api_name	No	String	API name.
env_id	No	String	Environment ID.
group_id	No	String	API group ID.
tags	No	String	API tag. Multiple API tags can be specified. The relationship between multiple parameter values is OR. If this parameter is not specified, no filtering tag is specified. If this parameter is set to #no_tags#, APIs without tags are filtered. Minimum: 0 Maximum: 128

Request Parameters

Table 4-771 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-772 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
apis	Array of UnbindApiForAcl objects	API list.

Table 4-773 UnbindApiForAcl

Parameter	Type	Description
id	String	API ID.
name	String	API name.
group_id	String	ID of the API group to which the API belongs.
group_name	String	Name of the API group to which the API belongs.
type	Integer	API visibility.
remark	String	API description.
run_env_name	String	Name of the environment in which the API has been published.
run_env_id	String	ID of the environment in which the API has been published.

Parameter	Type	Description
publish_id	String	API publication record ID.
acl_name	String	Name of the same type of access control policy bound to the API.
req_uri	String	API request address.
auth_type	String	API authentication mode.
req_method	String	Request method.
tags	Array of strings	Tags bound to the API. The default quota is 10. You can contact technical support to adjust the quota. Minimum: 1 Maximum: 128 Array Length: 0 - 10

Status code: 400**Table 4-774** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-775** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-776** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 404

Table 4-777 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-778 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total": 1,
  "size": 1,
  "apis": [ {
    "name": "Api_mock",
    "type": 1,
    "remark": "Mock backend API",
    "group_id": "c77f5e81d9cb4424bf704ef2b0ac7600",
    "id": "3a955b791bd24b1c9cd94c745f8d1aad",
    "group_name": "api_group_001",
    "run_env_name": "RELEASE",
    "run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "publish_id": "9f27d1dc4f4242a9abf88e563dbfc33d",
    "req_uri": "/test/mock",
    "auth_type": "IAM"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:api_name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3006",
  "error_msg" : "Access control policy 7eb619ecf2a24943b099833cd24a01ba does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.14.6 Querying Access Control Policies Bound to an API

Function

This API is used to query the access control policies that have been bound to a specified API.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/acl-bindings/binded-acls

Table 4-779 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-780 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
api_id	Yes	String	API ID.
env_id	No	String	Environment ID.
env_name	No	String	Environment name.
acl_id	No	String	Access control policy ID.
acl_name	No	String	Access control policy name.

Request Parameters

Table 4-781 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-782 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.

Parameter	Type	Description
acls	Array of ApiBindAclInfo objects	Access control policy list.

Table 4-783 ApiBindAclInfo

Parameter	Type	Description
acl_id	String	Access control policy ID.
acl_name	String	Access control policy name.
entity_type	String	Object type.
acl_type	String	Access control type. • PERMIT: whitelist • DENY: blacklist
acl_value	String	Access control objects.
env_id	String	Effective environment ID.
env_name	String	Effective environment name.
bind_id	String	Binding record ID.
bind_time	String	Binding time.

Status code: 400**Table 4-784** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-785** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-786** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-787** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-788** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "total" : 1,
  "size" : 1,
  "acls" : [ {
    "acl_id" : "7eb619ecf2a24943b099833cd24a01ba",
    "acl_name" : "acl_demo",
    "entity_type" : "IP",
    "acl_type" : "PERMIT",
    "acl_value" : "192.168.1.5,192.168.10.1",
    "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "env_name" : "RELEASE",
    "bind_id" : "332c5db1458a477b89b2ea741fec94a3",
    "bind_time" : "2020-08-04T08:58:03Z"
  }
]
```

```
  }]  
}
```

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2011",  
  "error_msg" : "Invalid parameter value,parameterName:acL_name. Please refer to the support  
documentation"  
}
```

Status code: 401

Unauthorized

```
{  
  "error_code" : "APIG.1002",  
  "error_msg" : "Incorrect token or token resolution failed"  
}
```

Status code: 403

Forbidden

```
{  
  "error_code" : "APIG.1005",  
  "error_msg" : "No permissions to request this method"  
}
```

Status code: 404

Not Found

```
{  
  "error_code" : "APIG.3002",  
  "error_msg" : "API 5f918d104dc84480a75166ba99efff21 does not exist"  
}
```

Status code: 500

Internal Server Error

```
{  
  "error_code" : "APIG.9999",  
  "error_msg" : "System error"  
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.15 Custom Authorizer Management

4.15.1 Creating a Custom Authorizer

Function

This API is used to create a custom authorizer.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/authorizers

Table 4-789 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-790 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-791 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Custom authorizer name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
type	Yes	String	Custom authorizer type. • FRONTEND • BACKEND Modification is not allowed.
authorizer_type	Yes	String	Value: FUNC.
authorizer_uri	Yes	String	Function URN.
network_type	No	String	Function network architecture: • V1: non-VPC • V2: VPC Default: V1
authorizer_version	No	String	Function version. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored. Maximum: 64
authorizer_alias_uri	No	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
identities	No	Array of Identity objects	Identity source.
ttl	No	Integer	Maximum cache age.
user_data	No	String	User data.
ld_api_id	No	String	Custom backend ID. Currently, this parameter is not supported.
need_body	No	Boolean	Indicates whether to send the body.

Table 4-792 Identity

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name.
location	Yes	String	Parameter location.
validation	No	String	Parameter verification expression. The default value is null, indicating that no verification is performed.

Response Parameters

Status code: 201

Table 4-793 Response body parameters

Parameter	Type	Description
name	String	Custom authorizer name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
type	String	Custom authorizer type. • FRONTEND • BACKEND Modification is not allowed.
authorizer_type	String	Value: FUNC.
authorizer_uri	String	Function URN.
network_type	String	Function network architecture: • V1: non-VPC • V2: VPC Default: V1
authorizer_version	String	Function version. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored. Maximum: 64

Parameter	Type	Description
authorizer_alias_uri	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
identities	Array of Identity objects	Identity source.
ttl	Integer	Maximum cache age.
user_data	String	User data.
ld_api_id	String	Custom backend ID. Currently, this parameter is not supported.
need_body	Boolean	Indicates whether to send the body.
id	String	Custom authorizer ID.
create_time	String	Creation time.
roma_app_id	String	ID of the application to which the custom authorizer belongs. Currently, this parameter is not supported.
roma_app_name	String	Name of the application to which the custom authorizer belongs. Currently, this parameter is not supported.

Table 4-794 Identity

Parameter	Type	Description
name	String	Parameter name.
location	String	Parameter location.
validation	String	Parameter verification expression. The default value is null, indicating that no verification is performed.

Status code: 400

Table 4-795 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-796** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-797** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-798** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-799** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Creating a frontend custom authorizer

```
{
  "name" : "Authorizer_demo",
  "type" : "FRONTEND",
  "authorizer_type" : "FUNC",
  "authorizer_uri" : "urn:fss:xx-xxx-4:106506b9a92342df9a5025fc12351cfc:function:default:apigDemo_1592617458814",
  "network_type" : "V1",
  "authorizer_version" : "v1",
  "authorizer_alias_uri" : "urn:fss:xx-xxx-4:106506b9a92342df9a5025fc12351cfc:function:default:apigDemo_1592617458814:v1",
  "identities" : [ {
    "name" : "header",
    "location" : "HEADER"
  } ],
  "user_data" : "authorizer_test"
}
```

Example Responses

Status code: 201

Created

```
{
  "name" : "Authorizer_demo",
  "type" : "FRONTEND",
  "authorizer_type" : "FUNC",
  "authorizer_uri" : "urn:fss:xx-xxx-4:106506b9a92342df9a5025fc12351cfc:function:default:apigDemo_1592617458814",
  "network_type" : "V1",
  "authorizer_version" : "v1",
  "authorizer_alias_uri" : "urn:fss:xx-xxx-4:106506b9a92342df9a5025fc12351cfc:function:default:apigDemo_1592617458814:v1",
  "identities" : [ {
    "name" : "header",
    "location" : "HEADER"
  } ],
  "ttl" : 0,
  "user_data" : "authorizer_test",
  "id" : "0d982c1ac3da493dae47627b6439fc5c",
  "create_time" : "2020-07-31T11:55:43Z"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:type. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden


```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3019",
  "error_msg" : "The function URN does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.15.2 Modifying a Custom Authorizer

Function

This API is used to modify a custom authorizer.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/authorizers/{authorizer_id}

Table 4-800 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
authorizer_id	Yes	String	Custom authorizer ID.

Request Parameters

Table 4-801 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-802 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Custom authorizer name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
type	Yes	String	Custom authorizer type. • FRONTEND • BACKEND Modification is not allowed.
authorizer_type	Yes	String	Value: FUNC.
authorizer_uri	Yes	String	Function URN.

Parameter	Mandatory	Type	Description
network_type	No	String	Function network architecture: • V1: non-VPC • V2: VPC Default: V1
authorizer_version	No	String	Function version. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored. Maximum: 64
authorizer_alias_uri	No	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
identities	No	Array of Identity objects	Identity source.
ttl	No	Integer	Maximum cache age.
user_data	No	String	User data.
ld_api_id	No	String	Custom backend ID. Currently, this parameter is not supported.
need_body	No	Boolean	Indicates whether to send the body.

Table 4-803 Identity

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name.
location	Yes	String	Parameter location.
validation	No	String	Parameter verification expression. The default value is null, indicating that no verification is performed.

Response Parameters

Status code: 200

Table 4-804 Response body parameters

Parameter	Type	Description
name	String	Custom authorizer name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
type	String	Custom authorizer type. • FRONTEND • BACKEND Modification is not allowed.
authorizer_type	String	Value: FUNC.
authorizer_uri	String	Function URN.
network_type	String	Function network architecture: • V1: non-VPC • V2: VPC Default: V1
authorizer_version	String	Function version. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored. Maximum: 64
authorizer_alias_uri	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
identities	Array of Identity objects	Identity source.
ttn	Integer	Maximum cache age.
user_data	String	User data.
ld_api_id	String	Custom backend ID. Currently, this parameter is not supported.
need_body	Boolean	Indicates whether to send the body.
id	String	Custom authorizer ID.
create_time	String	Creation time.

Parameter	Type	Description
roma_app_id	String	ID of the application to which the custom authorizer belongs. Currently, this parameter is not supported.
roma_app_name	String	Name of the application to which the custom authorizer belongs. Currently, this parameter is not supported.

Table 4-805 Identity

Parameter	Type	Description
name	String	Parameter name.
location	String	Parameter location.
validation	String	Parameter verification expression. The default value is null, indicating that no verification is performed.

Status code: 401**Table 4-806** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-807** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-808 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-809** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Updating a frontend custom authorizer

```
{
  "name" : "Authorizer_demo",
  "type" : "FRONTEND",
  "authorizer_type" : "FUNC",
  "authorizer_uri" : "urn:fss:xx-
xxx:106506b9a92342df9a5025fc12351cfc:function:default:apigDemo_1592617458814",
  "network_type" : "V1",
  "authorizer_version" : "v1",
  "authorizer_alias_uri" : "urn:fss:xx-
xxx-4:106506b9a92342df9a5025fc12351cfc:function:default:apigDemo_1592617458814:v1",
  "user_data" : "authorizer_test",
  "identities" : [ {
    "name" : "header",
    "location" : "HEADER"
  } ]
}
```

Example Responses

Status code: 200

OK

```
{
  "name" : "Authorizer_demo",
  "type" : "FRONTEND",
  "authorizer_type" : "FUNC",
  "authorizer_uri" : "urn:fss:xx-
xxx-4:106506b9a92342df9a5025fc12351cfc:function:default:apigDemo_1592617458814",
  "network_type" : "V1",
  "authorizer_version" : "v1",
  "authorizer_alias_uri" : "urn:fss:xx-
xxx-4:106506b9a92342df9a5025fc12351cfc:function:default:apigDemo_1592617458814:v1",
  "identities" : [ {
    "name" : "header",
    "location" : "HEADER"
  } ],
}
```

```
{
  "ttl" : 5,
  "user_data" : "authorizer_test",
  "id" : "0d982c1ac3da493dae47627b6439fc5c",
  "create_time" : "2020-07-08T03:27:52.000+0000"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3081",
  "error_msg" : "authorizer with id: 0d982c1ac3da493dae47627b6439fc5c not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.15.3 Deleting a Custom Authorizer

Function

This API is used to delete a custom authorizer.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/authorizers/{authorizer_id}

Table 4-810 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
authorizer_id	Yes	String	Custom authorizer ID.

Request Parameters

Table 4-811 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-812 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-813** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-814** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-815** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-816** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3081",
  "error_msg" : "authorizer with id: 0d982c1ac3da493dae47627b6439fc5c not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.15.4 Querying Custom Authorizer Details

Function

This API is used to query the details of a custom authorizer.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/authorizers/{authorizer_id}

Table 4-817 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
authorizer_id	Yes	String	Custom authorizer ID.

Request Parameters

Table 4-818 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-819** Response body parameters

Parameter	Type	Description
name	String	Custom authorizer name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
type	String	Custom authorizer type. • FRONTEND • BACKEND Modification is not allowed.
authorizer_type	String	Value: FUNC.
authorizer_uri	String	Function URN.
network_type	String	Function network architecture: • V1: non-VPC • V2: VPC Default: V1
authorizer_version	String	Function version. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored. Maximum: 64

Parameter	Type	Description
authorizer_alias_uri	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
identities	Array of Identity objects	Identity source.
ttn	Integer	Maximum cache age.
user_data	String	User data.
ld_api_id	String	Custom backend ID. Currently, this parameter is not supported.
need_body	Boolean	Indicates whether to send the body.
id	String	Custom authorizer ID.
create_time	String	Creation time.
roma_app_id	String	ID of the application to which the custom authorizer belongs. Currently, this parameter is not supported.
roma_app_name	String	Name of the application to which the custom authorizer belongs. Currently, this parameter is not supported.

Table 4-820 Identity

Parameter	Type	Description
name	String	Parameter name.
location	String	Parameter location.
validation	String	Parameter verification expression. The default value is null, indicating that no verification is performed.

Status code: 400

Table 4-821 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-822** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-823** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-824** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-825** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "name" : "Authorizer_demo",
  "type" : "FRONTEND",
  "authorizer_type" : "FUNC",
  "authorizer_uri" : "urn:fss:xx-xxx-4:106506b9a92342df9a5025fc12351cfc:function:default:apigDemo_1592617458814",
  "network_type" : "V1",
  "authorizer_version" : "v1",
  "authorizer_alias_uri" : "urn:fss:xx-xxx-4:106506b9a92342df9a5025fc12351cfc:function:default:apigDemo_1592617458814:v1",
  "identities" : [ {
    "name" : "header",
    "location" : "HEADER"
  } ],
  "ttl" : 0,
  "user_data" : "authorizer_test",
  "id" : "0d982c1ac3da493dae47627b6439fc5c",
  "create_time" : "2020-07-31T11:55:43Z"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:type. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3081",
  "error_msg" : "authorizer with id: 0d982c1ac3da493dae47627b6439fc5c not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.15.5 Querying Custom Authorizers

Function

This API is used to query all the custom authorizers under a gateway.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/authorizers

Table 4-826 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-827 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
id	No	String	ID.
name	No	String	Name.
type	No	String	Type.

Request Parameters

Table 4-828 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-829 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
authorizer_list	Array of AuthorizerResp objects	Custom authorizers.

Table 4-830 AuthorizerResp

Parameter	Type	Description
name	String	Custom authorizer name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
type	String	Custom authorizer type. • FRONTEND • BACKEND Modification is not allowed.
authorizer_type	String	Value: FUNC.
authorizer_uri	String	Function URN.
network_type	String	Function network architecture: • V1: non-VPC • V2: VPC Default: V1
authorizer_version	String	Function version. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored. Maximum: 64
authorizer_alias_uri	String	Function alias URN. If both a function alias URN and version are passed, the alias URN will be used and the version will be ignored.
identities	Array of Identity objects	Identity source.

Parameter	Type	Description
ttn	Integer	Maximum cache age.
user_data	String	User data.
ld_api_id	String	Custom backend ID. Currently, this parameter is not supported.
need_body	Boolean	Indicates whether to send the body.
id	String	Custom authorizer ID.
create_time	String	Creation time.
roma_app_id	String	ID of the application to which the custom authorizer belongs. Currently, this parameter is not supported.
roma_app_name	String	Name of the application to which the custom authorizer belongs. Currently, this parameter is not supported.

Table 4-831 Identity

Parameter	Type	Description
name	String	Parameter name.
location	String	Parameter location.
validation	String	Parameter verification expression. The default value is null, indicating that no verification is performed.

Status code: 400**Table 4-832** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-833 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-834** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-835** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-836** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{  
  "total" : 1,
```

```
"size" : 1,
"authorizer_list" : [ {
  "name" : "Authorizer_demo",
  "type" : "FRONTEND",
  "authorizer_type" : "FUNC",
  "authorizer_uri" : "urn:fss:xx-
xxx-4:106506b9a92342df9a5025fc12351cfc:function:default:apigDemo_1592617458814",
  "network_type" : "V1",
  "authorizer_version" : "v1",
  "authorizer_alias_uri" : "urn:fss:xx-
xxx-4:106506b9a92342df9a5025fc12351cfc:function:default:apigDemo_1592617458814:v1",
  "identities" : [ {
    "name" : "header",
    "location" : "HEADER"
  } ],
  "ttl" : 0,
  "user_data" : "authorizer_test",
  "id" : "0d982c1ac3da493dae47627b6439fc5c",
  "create_time" : "2020-07-31T11:55:43Z"
} ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.16 API Import and Export

4.16.1 Exporting APIs

Function

This API is used to export APIs in a specified API group. The content of the exported file complies with the Swagger standard. For details about the custom extended fields of APIG, see section "Importing and Exporting APIs" > "Extended Definition" in the API Gateway User Guide.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/openapi/export

Table 4-837 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-838 Query Parameters

Parameter	Mandatory	Type	Description
oas_version	No	String	Open API version. Default: 2.0

Request Parameters

Table 4-839 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-840 Request body parameters

Parameter	Mandatory	Type	Description
env_id	Yes	String	ID of the environment in which APIs of a group have been published.
group_id	Yes	String	API group ID.

Parameter	Mandatory	Type	Description
define	No	String	Definition scope of the APIs to be exported: • spec: basic definitions, including only the frontend definitions. • proxy: full definitions, including the frontend and backend definitions. • all: extended definitions, including the frontend and backend definitions as well as request throttling policies, access control policies, and custom authorizers. • dev: development definitions, including the frontend and backend definitions of APIs that have not been published. Default: spec
type	No	String	Format for exporting API definitions. Default: json
version	No	String	Version number of the APIs after exporting. The default value is the current date and time.
apis	No	Array of strings	IDs of the APIs to be exported.

Response Parameters

Status code: 200

Table 4-841 Response body parameters

Parameter	Type	Description
-	File	Exported API definition file, which is encoded in binary mode.

Status code: 400

Table 4-842 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-843** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-844** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-845** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-846** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Exporting APIs

```
{
  "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "define" : "all"
}
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2001",
  "error_msg" : "The request parameters must be specified,parameterName:env_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3001",
  "error_msg" : "API group c77f5e81d9cb4424bf704ef2b0ac7600 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK

Status Code	Description
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.16.2 Importing APIs

Function

This API is used to import APIs. The content of the imported file must comply with the Swagger standard. For details about the custom extended fields of APIG, see section "Importing and Exporting APIs" > "Extended Definition" in the API Gateway User Guide.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/openapi/import

Table 4-847 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-848 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-849 FormData parameters

Parameter	Mandatory	Type	Description
is_create_group	No	Boolean	Specifies whether to create an API group. Default: true
group_id	No	String	API group ID. This parameter is required when is_create_group is set to false .
extend_mode	No	String	Import mode of extended information. • merge: Retain the original extended information if a conflict occurs. • override: Override the original extended information if a conflict occurs. Default: merge
simple_mode	No	Boolean	Whether to enable fast import. Default: false
mock_mode	No	Boolean	Whether to enable the Mock backend. Default: false

Parameter	Mandatory	Type	Description
api_mode	No	String	Import mode. • merge: Retain the original API information if a conflict occurs. • override: Override the original API information if a conflict occurs. Default: merge
file_name	Yes	File	Request body in JSON, YAML, or YML format for importing APIs.

Response Parameters

Status code: 200

Table 4-850 Response body parameters

Parameter	Type	Description
success	Array of Success objects	Import success information.
failure	Array of Failure objects	Import failure information.
swagger	Swagger object	Swagger file import result. Currently, this parameter is not supported.
group_id	String	API group ID.
ignore	Array of Ignore objects	APIs that are not imported.

Table 4-851 Success

Parameter	Type	Description
path	String	API request path.
method	String	API request method.

Parameter	Type	Description
action	String	Import type. Options: • update: Update the APIs to an existing API group. • create: Create APIs for a new API group.
id	String	ID of a successfully imported API.

Table 4-852 Failure

Parameter	Type	Description
path	String	API request path.
error_msg	String	Error message displayed for an import failure.
method	String	API request method.
error_code	String	Error code displayed for an import failure.

Table 4-853 Swagger

Parameter	Type	Description
id	String	Swagger file No.
result	String	Import result description.

Table 4-854 Ignore

Parameter	Type	Description
method	String	API request method.
path	String	API request path.

Status code: 400**Table 4-855** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 401**Table 4-856** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-857** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-858** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-859** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Importing APIs

```
{
  "is_create_group" : false,
  "group_id" : "d9ce8c9eede54b3f841ec324fe0bfdc2",
  "file_name" : "APIGroup_test.json"
}
```

Example Responses

Status code: 200

OK

```
{
  "group_id" : "d9ce8c9eede54b3f841ec324fe0bfdc2",
  "failure" : [ {
    "path" : "/test/demo",
    "error_msg" : "The API already exists, An API with the same combination of the method, path, and x-
apigateway-match-mode fields already exists. API name: API_demo",
    "method" : "GET",
    "error_code" : "APIG.3301"
  } ],
  "success" : [ {
    "path" : "/test",
    "method" : "GET",
    "action" : "create",
    "id" : "8ae6bcfab6f49d78242bff26ad8a4f0"
  } ],
  "swagger" : {
    "id" : "e2ea8a7c1cfc49b3830437cb79d7fd59",
    "result" : "Success"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.3201",
  "error_msg" : "The API group name already exists"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found


```
{
  "error_code" : "APIG.3001",
  "error_msg" : "API group not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17 VPC Channel Management

4.17.1 Creating a VPC Channel

Function

This API is used to create a VPC channel from APIG to your private VPC resources. Afterwards, when creating an API, you can configure your backend service to use this VPC channel so that APIG can directly access your private VPC resources.

NOTE

You can create a maximum of 30 VPC channels.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels

Table 4-860 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-861 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-862 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	VPC channel name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
port	Yes	Integer	Host port of the VPC channel. Range: 1–65535.

Parameter	Mandatory	Type	Description
balance_strategy	Yes	Integer	Distribution algorithm. • 1: Weighted round robin (WRR). • 2: Weighted least connections (WLC). • 3: Source hashing. • 4: URI hashing. Default: 1
member_type	Yes	String	Member type of the VPC channel. • ip • ecs Default: ecs
type	No	Integer	VPC channel type. The default type is server. • 2: Server type • 3: Microservice type If vpc_channel_type is empty, the load balance channel type is determined by the type field. If the value of type is not 3 or the value of microservice_info is empty, the load balance channel type is server by default. If the value of type is 3 and the value of microservice_info is not empty, the load balance channel type is microservice. When you modify a load balance channel, the channel type will remain unchanged. This field is to be discarded. Use the vpc_channel_type field to specify the load balance channel type. Default: 2

Parameter	Mandatory	Type	Description
vpc_channel_type	No	String	VPC channel type. • builtin: server type • microservice: microservice type • reference: reference load balance channel If vpc_channel_type is empty, the load balance channel type depends on the value of the type field. If vpc_channel_type is non-empty and type is non-empty or non-zero, an error occurs when they are specified. If vpc_channel_type is non-empty and type is empty or 0, the value of vpc_channel_type is used to specify the load balance channel type. When you modify a load balance channel, the channel type will remain unchanged.
dict_code	No	String	Dictionary code of the VPC channel. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). This parameter is currently not supported. Minimum: 3 Maximum: 64
member_groups	No	Array of MemberGroupCreate objects	Backend server groups of the VPC channel. If service_type in microservice_info is set to NACOS, the weight of the server group cannot be manually set.
members	No	Array of MemberInfo objects	Backend instances of the VPC channel. This field will not be used to add or update backend instances for a reference load balance channel.

Parameter	Mandatory	Type	Description
vpc_health_config	No	VpcHealthConfig object	Health check details.
microservice_info	No	MicroServiceCreate object	Microservice details.

Table 4-863 MemberGroupCreate

Parameter	Mandatory	Type	Description
member_group_name	Yes	String	Name of the VPC channel's backend server group. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
member_group_remark	No	String	Description of the backend server group. Maximum: 255
member_group_weight	No	Integer	Weight of the backend server group. If the server group contains servers and a weight has been set for it, the weight is automatically used to assign weights to servers in this group. Minimum: 0 Maximum: 100
dict_code	No	String	Dictionary code of the backend server group. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). Currently, this parameter is not supported. Minimum: 3 Maximum: 64

Parameter	Mandatory	Type	Description
microservice_version	No	String	Version of the backend server group. This parameter is supported only when the VPC channel type is microservice. Maximum: 64
microservice_port	No	Integer	Port of the backend server group. This parameter is supported only when the VPC channel type is microservice. If the port number is 0, all addresses in the backend server group use the original load balancing port to inherit logic. Minimum: 0 Maximum: 65535
microservice_labels	No	Array of MicroserviceLabel objects	Tags of the backend server group. This parameter is supported only when the VPC channel type is microservice.
reference_vpc_channel_id	No	String	ID of the reference load balance channel. This parameter is supported only when the VPC channel type is reference (vpc_channel_type=reference). Minimum: 0 Maximum: 64

Table 4-864 MicroserviceLabel

Parameter	Mandatory	Type	Description
label_name	Yes	String	Tag name. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Parameter	Mandatory	Type	Description
label_value	Yes	String	Tag value. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Table 4-865 MemberInfo

Parameter	Mandatory	Type	Description
host	No	String	Backend server address. This parameter is required when the member type is IP address. Maximum: 255
weight	No	Integer	Weight. The higher the weight is, the more requests a backend service will receive. Minimum: 0 Maximum: 10000
is_backup	No	Boolean	Indicates whether the backend service is a standby node. After you enable this option, the corresponding backend service serves as the standby node and works only when all non-standby nodes are faulty. This function is supported only when your gateway has been upgraded to the corresponding version. If your gateway does not support this function, contact technical support. Default: false
member_group_name	No	String	Backend server group name. The server group facilitates backend service address modification.

Parameter	Mandatory	Type	Description
status	No	Integer	Backend server status. • 1: available • 2: unavailable
port	No	Integer	Backend server port. Minimum: 0 Maximum: 65535
ecs_id	No	String	Backend server ID. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), and underscores (_). Maximum: 255
ecs_name	No	String	Backend server name. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), underscores (_), and periods (.). Maximum: 64

Table 4-866 VpcHealthConfig

Parameter	Mandatory	Type	Description
protocol	Yes	String	Protocol for performing health checks on backend servers in the VPC channel. • TCP • HTTP • HTTPS
path	No	String	Destination path for health checks. This parameter is required if protocol is set to http or https.
method	No	String	Request method for health checks. Default: GET

Parameter	Mandatory	Type	Description
port	No	Integer	Destination port for health checks. If this parameter is not specified or set to 0, the host port of the VPC channel is used. If this parameter is set to a non-zero value, the corresponding port is used for health checks. Minimum: 0 Maximum: 65535
threshold_normal	Yes	Integer	Healthy threshold. It refers to the number of consecutive successful checks required for a backend server to be considered healthy. Minimum: 1 Maximum: 10
threshold_abnormal	Yes	Integer	Unhealthy threshold, which refers to the number of consecutive failed checks required for a backend server to be considered unhealthy. Minimum: 1 Maximum: 10
time_interval	Yes	Integer	Interval between consecutive checks. Unit: s. The value must be greater than the value of timeout. Minimum: 1 Maximum: 300

Parameter	Mandatory	Type	Description
http_code	No	String	Response codes for determining a successful HTTP response. The value can be any integer within 100–599 in one of the following formats: • Multiple values, for example, 200,201,202 • Range, for example, 200-299 • Multiple values and ranges, for example, 201,202,210-299. This parameter is required if protocol is set to http.
enable_client_ssl	No	Boolean	Indicates whether to enable two-way authentication. If this function is enabled, the certificate specified in the backend_client_certificate configuration item of the instance is used. Default: false
status	No	Integer	Health check result. • 1: available • 2: unavailable
timeout	Yes	Integer	Timeout for determining whether a health check fails. Unit: s. The value must be less than the value of time_interval. Minimum: 1 Maximum: 30

Table 4-867 MicroServiceCreate

Parameter	Mandatory	Type	Description
service_type	No	String	Microservice type. • CSE: CSE microservice registration center. • CCE: CCE workload • CCE_SERVICE: CCE Service (not supported currently) • NACOS: Nacos registration center. nacos_info is mandatory.
cse_info	No	MicroServiceInfoCSEBase object	CSE microservice details. This parameter is required if service_type is set to CSE.
cce_info	No	MicroServiceInfoCCEBase object	CCE workload details. This parameter is required if service_type is set to CCE. Either app_name or any of label_key and label_value must be set. If only app_name is set, label_key='app' and label_value=app_name.
cce_service_info	No	MicroServiceInfoCCEServiceBase object	CCE Service details.
nacos_info	No	MicroServiceInfoNacosBase object	Nacos basic information.

Table 4-868 MicroServiceInfoCSEBase

Parameter	Mandatory	Type	Description
engine_id	Yes	String	Microservice engine ID. Maximum: 64
service_id	Yes	String	Microservice ID. Maximum: 64

Table 4-869 MicroServiceInfoCCEBase

Parameter	Mandatory	Type	Description
cluster_id	Yes	String	CCE cluster ID. Maximum: 64
namespace	Yes	String	Namespace. Maximum: 64
workload_type	Yes	String	Workload type. • deployment • statefulset • daemonset
app_name	No	String	App name. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
label_key	No	String	Service label key. Start with a letter or digit, and use only letters, digits, and these special characters: -_/:(). (1 to 64 characters) Minimum: 1 Maximum: 64
label_value	No	String	Service label value. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64

Table 4-870 MicroServiceInfoCCEServiceBase

Parameter	Mandatory	Type	Description
cluster_id	Yes	String	CCE cluster ID. Maximum: 64

Parameter	Mandatory	Type	Description
namespace	Yes	String	Namespace. 1 to 63 characters. Use lowercase letters, digits, and hyphens (-). Start with a letter and end with a letter or digit. Minimum: 1 Maximum: 63
service_name	Yes	String	Service name. Start with a letter, and use only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64

Table 4-871 MicroServiceInfoNacosBase

Parameter	Mandatory	Type	Description
namespace	No	String	Namespace ID. If the default namespace public is used, leave this parameter empty. Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
cluster_name	No	String	Cluster name. The default value is DEFAULT . Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
group_name	No	String	Group name. The default value is DEFAULT_GROUP . Only letters, numbers, hyphens (-), underscores (_), periods (.), and colons (:) are allowed. Max.: 128 characters Minimum: 0 Maximum: 128

Parameter	Mandatory	Type	Description
service_name	Yes	String	Microservice name. The value cannot start with @ or contain @@. Max.: 512 characters Minimum: 1 Maximum: 512
server_config	Yes	Array of NacosServerConfig objects	Nacos server configurations. Array Length: 1 - 9
user_info	Yes	NacosUserInfo object	Nacos user information.

Table 4-872 NacosServerConfig

Parameter	Mandatory	Type	Description
ip_address	Yes	String	IP address of the Nacos server. Minimum: 7 Maximum: 128
port	Yes	Integer	Port number of the Nacos server. Range: 1–65535. Minimum: 1 Maximum: 65535
grpc_port	No	Integer	gRPC port number of the Nacos server. Default: port number + 1000 Range: 1–65535. Minimum: 1 Maximum: 65535

Table 4-873 NacosUserInfo

Parameter	Mandatory	Type	Description
user_name	Yes	String	Nacos username. Minimum: 1 Maximum: 64
password	Yes	String	Nacos password. Minimum: 1 Maximum: 64

Response Parameters

Status code: 201

Table 4-874 Response body parameters

Parameter	Type	Description
name	String	VPC channel name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
port	Integer	Host port of the VPC channel. Range: 1-65535.
balance_strategy	Integer	Distribution algorithm. • 1: Weighted round robin (WRR). • 2: Weighted least connections (WLC). • 3: Source hashing. • 4: URI hashing. Default: 1
member_type	String	Member type of the VPC channel. • ip • ecs Default: ecs

Parameter	Type	Description
type	Integer	VPC channel type. The default type is server. • 2: Server type • 3: Microservice type If vpc_channel_type is empty, the load balance channel type is determined by the type field. If the value of type is not 3 or the value of microservice_info is empty, the load balance channel type is server by default. If the value of type is 3 and the value of microservice_info is not empty, the load balance channel type is microservice. When you modify a load balance channel, the channel type will remain unchanged. This field is to be discarded. Use the vpc_channel_type field to specify the load balance channel type. Default: 2
vpc_channel_type	String	VPC channel type. • builtin: server type • microservice: microservice type • reference: reference load balance channel If vpc_channel_type is empty, the load balance channel type depends on the value of the type field. If vpc_channel_type is non-empty and type is non-empty or non-zero, an error occurs when they are specified. If vpc_channel_type is non-empty and type is empty or 0, the value of vpc_channel_type is used to specify the load balance channel type. When you modify a load balance channel, the channel type will remain unchanged.

Parameter	Type	Description
dict_code	String	Dictionary code of the VPC channel. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). This parameter is currently not supported. Minimum: 3 Maximum: 64
create_time	String	Time when the VPC channel is created.
id	String	VPC channel ID.
status	Integer	VPC channel status. • 1: normal • 2: abnormal
member_groups	Array of MemberGroupInfo objects	Backend server groups.
microservice_info	MicroServiceInfo object	Microservice information.

Table 4-875 MemberGroupInfo

Parameter	Type	Description
member_group_name	String	Name of the VPC channel's backend server group. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
member_group_remark	String	Description of the backend server group. Maximum: 255
member_group_weight	Integer	Weight of the backend server group. If the server group contains servers and a weight has been set for it, the weight is automatically used to assign weights to servers in this group. Minimum: 0 Maximum: 100

Parameter	Type	Description
dict_code	String	Dictionary code of the backend server group. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). Currently, this parameter is not supported. Minimum: 3 Maximum: 64
microservice_version	String	Version of the backend server group. This parameter is supported only when the VPC channel type is microservice. Maximum: 64
microservice_port	Integer	Port of the backend server group. This parameter is supported only when the VPC channel type is microservice. If the port number is 0, all addresses in the backend server group use the original load balancing port to inherit logic. Minimum: 0 Maximum: 65535
microservice_labels	Array of MicroserviceLabel objects	Tags of the backend server group. This parameter is supported only when the VPC channel type is microservice.
reference_vpc_channel_id	String	ID of the reference load balance channel. This parameter is supported only when the VPC channel type is reference (vpc_channel_type=reference). Minimum: 0 Maximum: 64
member_group_id	String	ID of the backend server group of the VPC channel.
create_time	String	Time when the backend server group is created.
update_time	String	Time when the backend server group is updated.

Table 4-876 MicroserviceLabel

Parameter	Type	Description
label_name	String	Tag name. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63
label_value	String	Tag value. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Table 4-877 MicroServiceInfo

Parameter	Type	Description
id	String	Microservice ID.
instance_id	String	Gateway ID.
service_type	String	Microservice type. • CSE: CSE microservice registration center. • CCE: CCE workload • CCE_SERVICE: CCE Service (not supported currently) • NACOS: Nacos engine. nacos_info is mandatory.
cse_info	MicroServiceInfo CSE object	CSE microservice details.
cce_info	MicroServiceInfo CCE object	CCE microservice workload details.
cce_service_info	MicroServiceInfo CCEService object	CCE microservice Service details.
nacos_info	MicroServiceInfo-NacosBase object	Nacos basic information.
update_time	String	Microservice update time.

Parameter	Type	Description
create_time	String	Microservice creation time.

Table 4-878 MicroServiceInfoCSE

Parameter	Type	Description
engine_id	String	Microservice engine ID. Maximum: 64
service_id	String	Microservice ID. Maximum: 64
engine_name	String	Microservice engine name.
service_name	String	Microservice name.
register_address	String	Registration center address.
cse_app_id	String	App to which the microservice belongs.
version	String	Microservice version, which has been discarded and is reflected in the version of the backend server group. Maximum: 64

Table 4-879 MicroServiceInfoCCE

Parameter	Type	Description
cluster_id	String	CCE cluster ID. Maximum: 64
namespace	String	Namespace. Maximum: 64
workload_type	String	Workload type. • deployment • statefulset • daemonset
app_name	String	App name. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64

Parameter	Type	Description
label_key	String	Service label key. Start with a letter or digit, and use only letters, digits, and these special characters: -_/:(). (1 to 64 characters) Minimum: 1 Maximum: 64
label_value	String	Service label value. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
cluster_name	String	CCE cluster name.

Table 4-880 MicroServiceInfoCCEService

Parameter	Type	Description
cluster_id	String	CCE cluster ID. Maximum: 64
namespace	String	Namespace. 1 to 63 characters. Use lowercase letters, digits, and hyphens (-). Start with a letter and end with a letter or digit. Minimum: 1 Maximum: 63
service_name	String	Service name. Start with a letter, and use only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
cluster_name	String	CCE cluster name.

Table 4-881 MicroServiceInfoNacosBase

Parameter	Type	Description
namespace	String	Namespace ID. If the default namespace public is used, leave this parameter empty. Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
cluster_name	String	Cluster name. The default value is DEFAULT . Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
group_name	String	Group name. The default value is DEFAULT_GROUP . Only letters, numbers, hyphens (-), underscores (_), periods (.), and colons (:) are allowed. Max.: 128 characters Minimum: 0 Maximum: 128
service_name	String	Microservice name. The value cannot start with @ or contain @@. Max.: 512 characters Minimum: 1 Maximum: 512
server_config	Array of NacosServerConfig objects	Nacos server configurations. Array Length: 1 - 9
user_info	NacosUserInfo object	Nacos user information.

Table 4-882 NacosServerConfig

Parameter	Type	Description
ip_address	String	IP address of the Nacos server. Minimum: 7 Maximum: 128

Parameter	Type	Description
port	Integer	Port number of the Nacos server. Range: 1–65535. Minimum: 1 Maximum: 65535
grpc_port	Integer	gRPC port number of the Nacos server. Default: port number + 1000 Range: 1–65535. Minimum: 1 Maximum: 65535

Table 4-883 NacosUserInfo

Parameter	Type	Description
user_name	String	Nacos username. Minimum: 1 Maximum: 64
password	String	Nacos password. Minimum: 1 Maximum: 64

Status code: 400**Table 4-884** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-885** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-886** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-887** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-888** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

- Creating a VPC channel of the server type

```
{
  "balance_strategy" : 1,
  "member_type" : "ip",
  "name" : "VPC_demo",
  "port" : 22,
  "type" : 2,
  "vpc_health_config" : {
    "http_code" : "200",
    "path" : "/vpc/demo",
    "port" : 22,
    "protocol" : "http",
    "threshold_abnormal" : 5,
    "threshold_normal" : 2,
    "time_interval" : 10,
    "timeout" : 5,
    "enable_client_ssl" : false
  },
  "member_groups" : [ {
    "member_group_name" : "test",
    "member_group_weight" : 1,
    "member_group_remark" : "remark"
  } ]
}
```



```
}, {  
  "member_group_name": "default",  
  "member_group_weight": 2,  
  "member_group_remark": "remark"  
}],  
"members": [ {  
  "host": "192.168.0.5",  
  "weight": 1,  
  "member_group_name": "test"  
}, {  
  "host": "192.168.1.124",  
  "weight": 2,  
  "member_group_name": "default"  
}]  
}
```

- Creating a VPC channel of the microservice type

```
{  
  "balance_strategy": 1,  
  "member_type": "ip",  
  "name": "VPC_demo",  
  "port": 22,  
  "type": 3,  
  "vpc_health_config": {  
    "http_code": "200",  
    "path": "/vpc/demo",  
    "port": 22,  
    "protocol": "http",  
    "threshold_abnormal": 5,  
    "threshold_normal": 2,  
    "time_interval": 10,  
    "timeout": 5,  
    "enable_client_ssl": false  
  },  
  "member_groups": [ {  
    "member_group_name": "test",  
    "member_group_weight": 1,  
    "member_group_remark": "remark",  
    "microservice_version": "v1",  
    "microservice_port": 80  
  }, {  
    "member_group_name": "default",  
    "member_group_weight": 2,  
    "member_group_remark": "remark",  
    "microservice_version": "v2",  
    "microservice_port": 80,  
    "microservice_labels": [ {  
      "label_name": "cluster_id",  
      "label_value": "c429700c-5dc4-482a-9c0e-99f6c0635113"  
    } ]  
  } ],  
  "members": [ {  
    "host": "192.168.0.5",  
    "weight": 1,  
    "member_group_name": "test"  
  }, {  
    "host": "192.168.1.124",  
    "weight": 2,  
    "member_group_name": "default"  
  } ],  
  "microservice_info": {  
    "service_type": "CCE",  
    "cce_info": {  
      "cluster_id": "ab1485b4f91b45abbcd560be591f7309",  
      "namespace": "default",  
      "workload_type": "deployment",  
      "app_name": "testapp"  
    }  
  }  
}
```

Example Responses

Status code: 201

Created

- Example 1

```
{
  "name": "VPC_demo",
  "id": "105c6902457144a4820dff8b1ad63331",
  "balance_strategy": 1,
  "dict_code": "",
  "create_time": "2020-07-23T07:11:57.244829604Z",
  "member_type": "ip",
  "port": 22,
  "status": 1,
  "member_groups": [ {
    "member_group_id": "c1ce135c705c4066853a0460b318fe16",
    "member_group_name": "test",
    "member_group_weight": 1,
    "member_group_remark": "remark",
    "create_time": "2020-07-23T07:11:57.244829604Z",
    "update_time": "2020-07-23T07:11:57.244829604Z",
    "microservice_version": "",
    "microservice_port": 0
  }, {
    "member_group_id": "c1ce135c705c4066853a0460b318fe17",
    "member_group_name": "default",
    "member_group_weight": 2,
    "member_group_remark": "remark",
    "create_time": "2020-07-23T07:11:57.244829604Z",
    "update_time": "2020-07-23T07:11:57.244829604Z",
    "microservice_version": "",
    "microservice_port": 0
  } ],
  "type": 2,
  "microservice_info": {
    "id": "",
    "instance_id": "",
    "service_type": "",
    "cse_info": {
      "cse_app_id": "",
      "engine_id": "",
      "engine_name": "",
      "register_address": "",
      "service_id": "",
      "service_name": ""
    },
    "cce_info": {
      "cluster_id": "",
      "cluster_name": "",
      "namespace": "",
      "workload_type": "",
      "app_name": ""
    },
    "create_time": "",
    "update_time": ""
  }
}
```

- Example 2

```
{
  "name": "VPC_demo",
  "id": "105c6902457144a4820dff8b1ad63331",
  "balance_strategy": 1,
  "dict_code": "",
  "create_time": "2020-07-23T07:11:57.244829604Z",
  "member_type": "ip",
}
```

```
"port" : 22,
"status" : 1,
"member_groups" : [ {
  "member_group_id" : "c1ce135c705c4066853a0460b318fe16",
  "member_group_name" : "test",
  "member_group_weight" : 1,
  "member_group_remark" : "remark",
  "create_time" : "2020-07-23T07:11:57.244829604Z",
  "update_time" : "2020-07-23T07:11:57.244829604Z",
  "microservice_version" : "v1",
  "microservice_port" : 80
}, {
  "member_group_id" : "c1ce135c705c4066853a0460b318fe17",
  "member_group_name" : "default",
  "member_group_weight" : 2,
  "member_group_remark" : "remark",
  "create_time" : "2020-07-23T07:11:57.244829604Z",
  "update_time" : "2020-07-23T07:11:57.244829604Z",
  "microservice_version" : "v2",
  "microservice_port" : 80,
  "microservice_labels" : [ {
    "label_name" : "cluster_id",
    "label_value" : "c429700c-5dc4-482a-9c0e-99f6c0635113"
  } ]
}],
"type" : 3,
"microservice_info" : {
  "id" : "9483afa235be45158a70c19ab817ac65",
  "instance_id" : "eddc4d25480b4cd6b512f270a1b8b341",
  "service_type" : "CCE",
  "cse_info" : {
    "cse_app_id" : "",
    "engine_id" : "",
    "engine_name" : "",
    "register_address" : "",
    "service_id" : "",
    "service_name" : ""
  },
  "cce_info" : {
    "cluster_id" : "ab1485b4f91b45abbcd560be591f7309",
    "cluster_name" : "cce-test",
    "namespace" : "default",
    "workload_type" : "deployment",
    "app_name" : "testapp"
  },
  "create_time" : "2020-07-23T07:11:57.244829604Z",
  "update_time" : "2020-07-23T07:11:57.244829604Z"
}
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2001",
  "error_msg" : "The request parameters must be specified, parameter name:members"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.2 Updating a VPC Channel

Function

This API is used to update parameters of a specified VPC channel.

If the VPC channel is overwritten with an empty backend instance list, all the existing backend instances will be deleted.

If the VPC channel is overwritten with an empty backend server group list, all the existing backend server groups will be deleted.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}

Table 4-889 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
vpc_channel_id	Yes	String	VPC channel ID.

Request Parameters

Table 4-890 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-891 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	VPC channel name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
port	Yes	Integer	Host port of the VPC channel. Range: 1–65535.

Parameter	Mandatory	Type	Description
balance_strategy	Yes	Integer	Distribution algorithm. • 1: Weighted round robin (WRR). • 2: Weighted least connections (WLC). • 3: Source hashing. • 4: URI hashing. Default: 1
member_type	Yes	String	Member type of the VPC channel. • ip • ecs Default: ecs
type	No	Integer	VPC channel type. The default type is server. • 2: Server type • 3: Microservice type If vpc_channel_type is empty, the load balance channel type is determined by the type field. If the value of type is not 3 or the value of microservice_info is empty, the load balance channel type is server by default. If the value of type is 3 and the value of microservice_info is not empty, the load balance channel type is microservice. When you modify a load balance channel, the channel type will remain unchanged. This field is to be discarded. Use the vpc_channel_type field to specify the load balance channel type. Default: 2

Parameter	Mandatory	Type	Description
vpc_channel_type	No	String	VPC channel type. • builtin: server type • microservice: microservice type • reference: reference load balance channel If vpc_channel_type is empty, the load balance channel type depends on the value of the type field. If vpc_channel_type is non-empty and type is non-empty or non-zero, an error occurs when they are specified. If vpc_channel_type is non-empty and type is empty or 0, the value of vpc_channel_type is used to specify the load balance channel type. When you modify a load balance channel, the channel type will remain unchanged.
dict_code	No	String	Dictionary code of the VPC channel. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). This parameter is currently not supported. Minimum: 3 Maximum: 64
member_groups	No	Array of MemberGroupCreate objects	Backend server groups of the VPC channel. If service_type in microservice_info is set to NACOS, the weight of the server group cannot be manually set.
members	No	Array of MemberInfo objects	Backend instances of the VPC channel. This field will not be used to add or update backend instances for a reference load balance channel.

Parameter	Mandatory	Type	Description
vpc_health_config	No	VpcHealthConfig object	Health check details.
microservice_info	No	MicroServiceCreate object	Microservice details.

Table 4-892 MemberGroupCreate

Parameter	Mandatory	Type	Description
member_group_name	Yes	String	Name of the VPC channel's backend server group. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
member_group_remark	No	String	Description of the backend server group. Maximum: 255
member_group_weight	No	Integer	Weight of the backend server group. If the server group contains servers and a weight has been set for it, the weight is automatically used to assign weights to servers in this group. Minimum: 0 Maximum: 100
dict_code	No	String	Dictionary code of the backend server group. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). Currently, this parameter is not supported. Minimum: 3 Maximum: 64

Parameter	Mandatory	Type	Description
microservice_version	No	String	Version of the backend server group. This parameter is supported only when the VPC channel type is microservice. Maximum: 64
microservice_port	No	Integer	Port of the backend server group. This parameter is supported only when the VPC channel type is microservice. If the port number is 0, all addresses in the backend server group use the original load balancing port to inherit logic. Minimum: 0 Maximum: 65535
microservice_labels	No	Array of MicroserviceLabel objects	Tags of the backend server group. This parameter is supported only when the VPC channel type is microservice.
reference_vpc_channel_id	No	String	ID of the reference load balance channel. This parameter is supported only when the VPC channel type is reference (vpc_channel_type=reference). Minimum: 0 Maximum: 64

Table 4-893 MicroserviceLabel

Parameter	Mandatory	Type	Description
label_name	Yes	String	Tag name. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Parameter	Mandatory	Type	Description
label_value	Yes	String	Tag value. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Table 4-894 MemberInfo

Parameter	Mandatory	Type	Description
host	No	String	Backend server address. This parameter is required when the member type is IP address. Maximum: 255
weight	No	Integer	Weight. The higher the weight is, the more requests a backend service will receive. Minimum: 0 Maximum: 10000
is_backup	No	Boolean	Indicates whether the backend service is a standby node. After you enable this option, the corresponding backend service serves as the standby node and works only when all non-standby nodes are faulty. This function is supported only when your gateway has been upgraded to the corresponding version. If your gateway does not support this function, contact technical support. Default: false
member_group_name	No	String	Backend server group name. The server group facilitates backend service address modification.

Parameter	Mandatory	Type	Description
status	No	Integer	Backend server status. • 1: available • 2: unavailable
port	No	Integer	Backend server port. Minimum: 0 Maximum: 65535
ecs_id	No	String	Backend server ID. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), and underscores (_). Maximum: 255
ecs_name	No	String	Backend server name. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), underscores (_), and periods (.). Maximum: 64

Table 4-895 VpcHealthConfig

Parameter	Mandatory	Type	Description
protocol	Yes	String	Protocol for performing health checks on backend servers in the VPC channel. • TCP • HTTP • HTTPS
path	No	String	Destination path for health checks. This parameter is required if protocol is set to http or https.
method	No	String	Request method for health checks. Default: GET

Parameter	Mandatory	Type	Description
port	No	Integer	Destination port for health checks. If this parameter is not specified or set to 0, the host port of the VPC channel is used. If this parameter is set to a non-zero value, the corresponding port is used for health checks. Minimum: 0 Maximum: 65535
threshold_normal	Yes	Integer	Healthy threshold. It refers to the number of consecutive successful checks required for a backend server to be considered healthy. Minimum: 1 Maximum: 10
threshold_abnormal	Yes	Integer	Unhealthy threshold, which refers to the number of consecutive failed checks required for a backend server to be considered unhealthy. Minimum: 1 Maximum: 10
time_interval	Yes	Integer	Interval between consecutive checks. Unit: s. The value must be greater than the value of timeout. Minimum: 1 Maximum: 300

Parameter	Mandatory	Type	Description
http_code	No	String	Response codes for determining a successful HTTP response. The value can be any integer within 100–599 in one of the following formats: • Multiple values, for example, 200,201,202 • Range, for example, 200-299 • Multiple values and ranges, for example, 201,202,210-299. This parameter is required if protocol is set to http.
enable_client_ssl	No	Boolean	Indicates whether to enable two-way authentication. If this function is enabled, the certificate specified in the backend_client_certificate configuration item of the instance is used. Default: false
status	No	Integer	Health check result. • 1: available • 2: unavailable
timeout	Yes	Integer	Timeout for determining whether a health check fails. Unit: s. The value must be less than the value of time_interval. Minimum: 1 Maximum: 30

Table 4-896 MicroServiceCreate

Parameter	Mandatory	Type	Description
service_type	No	String	Microservice type. • CSE: CSE microservice registration center. • CCE: CCE workload • CCE_SERVICE: CCE Service (not supported currently) • NACOS: Nacos registration center. nacos_info is mandatory.
cse_info	No	MicroServiceInfoCSEBase object	CSE microservice details. This parameter is required if service_type is set to CSE.
cce_info	No	MicroServiceInfoCCEBase object	CCE workload details. This parameter is required if service_type is set to CCE. Either app_name or any of label_key and label_value must be set. If only app_name is set, label_key='app' and label_value=app_name.
cce_service_info	No	MicroServiceInfoCCEServiceBase object	CCE Service details.
nacos_info	No	MicroServiceInfoNacosBase object	Nacos basic information.

Table 4-897 MicroServiceInfoCSEBase

Parameter	Mandatory	Type	Description
engine_id	Yes	String	Microservice engine ID. Maximum: 64
service_id	Yes	String	Microservice ID. Maximum: 64

Table 4-898 MicroServiceInfoCCEBase

Parameter	Mandatory	Type	Description
cluster_id	Yes	String	CCE cluster ID. Maximum: 64
namespace	Yes	String	Namespace. Maximum: 64
workload_type	Yes	String	Workload type. • deployment • statefulset • daemonset
app_name	No	String	App name. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
label_key	No	String	Service label key. Start with a letter or digit, and use only letters, digits, and these special characters: -_/:(). (1 to 64 characters) Minimum: 1 Maximum: 64
label_value	No	String	Service label value. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64

Table 4-899 MicroServiceInfoCCEServiceBase

Parameter	Mandatory	Type	Description
cluster_id	Yes	String	CCE cluster ID. Maximum: 64

Parameter	Mandatory	Type	Description
namespace	Yes	String	Namespace. 1 to 63 characters. Use lowercase letters, digits, and hyphens (-). Start with a letter and end with a letter or digit. Minimum: 1 Maximum: 63
service_name	Yes	String	Service name. Start with a letter, and use only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64

Table 4-900 MicroServiceInfoNacosBase

Parameter	Mandatory	Type	Description
namespace	No	String	Namespace ID. If the default namespace public is used, leave this parameter empty. Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
cluster_name	No	String	Cluster name. The default value is DEFAULT . Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
group_name	No	String	Group name. The default value is DEFAULT_GROUP . Only letters, numbers, hyphens (-), underscores (_), periods (.), and colons (:) are allowed. Max.: 128 characters Minimum: 0 Maximum: 128

Parameter	Mandatory	Type	Description
service_name	Yes	String	Microservice name. The value cannot start with @ or contain @@. Max.: 512 characters Minimum: 1 Maximum: 512
server_config	Yes	Array of NacosServerConfig objects	Nacos server configurations. Array Length: 1 - 9
user_info	Yes	NacosUserInfo object	Nacos user information.

Table 4-901 NacosServerConfig

Parameter	Mandatory	Type	Description
ip_address	Yes	String	IP address of the Nacos server. Minimum: 7 Maximum: 128
port	Yes	Integer	Port number of the Nacos server. Range: 1–65535. Minimum: 1 Maximum: 65535
grpc_port	No	Integer	gRPC port number of the Nacos server. Default: port number + 1000 Range: 1–65535. Minimum: 1 Maximum: 65535

Table 4-902 NacosUserInfo

Parameter	Mandatory	Type	Description
user_name	Yes	String	Nacos username. Minimum: 1 Maximum: 64
password	Yes	String	Nacos password. Minimum: 1 Maximum: 64

Response Parameters

Status code: 200

Table 4-903 Response body parameters

Parameter	Type	Description
name	String	VPC channel name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
port	Integer	Host port of the VPC channel. Range: 1-65535.
balance_strategy	Integer	Distribution algorithm. • 1: Weighted round robin (WRR). • 2: Weighted least connections (WLC). • 3: Source hashing. • 4: URI hashing. Default: 1
member_type	String	Member type of the VPC channel. • ip • ecs Default: ecs

Parameter	Type	Description
type	Integer	VPC channel type. The default type is server. • 2: Server type • 3: Microservice type If vpc_channel_type is empty, the load balance channel type is determined by the type field. If the value of type is not 3 or the value of microservice_info is empty, the load balance channel type is server by default. If the value of type is 3 and the value of microservice_info is not empty, the load balance channel type is microservice. When you modify a load balance channel, the channel type will remain unchanged. This field is to be discarded. Use the vpc_channel_type field to specify the load balance channel type. Default: 2
vpc_channel_type	String	VPC channel type. • builtin: server type • microservice: microservice type • reference: reference load balance channel If vpc_channel_type is empty, the load balance channel type depends on the value of the type field. If vpc_channel_type is non-empty and type is non-empty or non-zero, an error occurs when they are specified. If vpc_channel_type is non-empty and type is empty or 0, the value of vpc_channel_type is used to specify the load balance channel type. When you modify a load balance channel, the channel type will remain unchanged.

Parameter	Type	Description
dict_code	String	Dictionary code of the VPC channel. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). This parameter is currently not supported. Minimum: 3 Maximum: 64
create_time	String	Time when the VPC channel is created.
id	String	VPC channel ID.
status	Integer	VPC channel status. • 1: normal • 2: abnormal
member_groups	Array of MemberGroupInfo objects	Backend server groups.
microservice_info	MicroServiceInfo object	Microservice information.

Table 4-904 MemberGroupInfo

Parameter	Type	Description
member_group_name	String	Name of the VPC channel's backend server group. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
member_group_remark	String	Description of the backend server group. Maximum: 255
member_group_weight	Integer	Weight of the backend server group. If the server group contains servers and a weight has been set for it, the weight is automatically used to assign weights to servers in this group. Minimum: 0 Maximum: 100

Parameter	Type	Description
dict_code	String	Dictionary code of the backend server group. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). Currently, this parameter is not supported. Minimum: 3 Maximum: 64
microservice_version	String	Version of the backend server group. This parameter is supported only when the VPC channel type is microservice. Maximum: 64
microservice_port	Integer	Port of the backend server group. This parameter is supported only when the VPC channel type is microservice. If the port number is 0, all addresses in the backend server group use the original load balancing port to inherit logic. Minimum: 0 Maximum: 65535
microservice_labels	Array of MicroserviceLabel objects	Tags of the backend server group. This parameter is supported only when the VPC channel type is microservice.
reference_vpc_channel_id	String	ID of the reference load balance channel. This parameter is supported only when the VPC channel type is reference (vpc_channel_type=reference). Minimum: 0 Maximum: 64
member_group_id	String	ID of the backend server group of the VPC channel.
create_time	String	Time when the backend server group is created.
update_time	String	Time when the backend server group is updated.

Table 4-905 MicroserviceLabel

Parameter	Type	Description
label_name	String	Tag name. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63
label_value	String	Tag value. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Table 4-906 MicroServiceInfo

Parameter	Type	Description
id	String	Microservice ID.
instance_id	String	Gateway ID.
service_type	String	Microservice type. • CSE: CSE microservice registration center. • CCE: CCE workload • CCE_SERVICE: CCE Service (not supported currently) • NACOS: Nacos engine. nacos_info is mandatory.
cse_info	MicroServiceInfo CSE object	CSE microservice details.
cce_info	MicroServiceInfo CCE object	CCE microservice workload details.
cce_service_info	MicroServiceInfo CCEService object	CCE microservice Service details.
nacos_info	MicroServiceInfo-NacosBase object	Nacos basic information.
update_time	String	Microservice update time.

Parameter	Type	Description
create_time	String	Microservice creation time.

Table 4-907 MicroServiceInfoCSE

Parameter	Type	Description
engine_id	String	Microservice engine ID. Maximum: 64
service_id	String	Microservice ID. Maximum: 64
engine_name	String	Microservice engine name.
service_name	String	Microservice name.
register_address	String	Registration center address.
cse_app_id	String	App to which the microservice belongs.
version	String	Microservice version, which has been discarded and is reflected in the version of the backend server group. Maximum: 64

Table 4-908 MicroServiceInfoCCE

Parameter	Type	Description
cluster_id	String	CCE cluster ID. Maximum: 64
namespace	String	Namespace. Maximum: 64
workload_type	String	Workload type. • deployment • statefulset • daemonset
app_name	String	App name. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64

Parameter	Type	Description
label_key	String	Service label key. Start with a letter or digit, and use only letters, digits, and these special characters: -_/:(). (1 to 64 characters) Minimum: 1 Maximum: 64
label_value	String	Service label value. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
cluster_name	String	CCE cluster name.

Table 4-909 MicroServiceInfoCCEService

Parameter	Type	Description
cluster_id	String	CCE cluster ID. Maximum: 64
namespace	String	Namespace. 1 to 63 characters. Use lowercase letters, digits, and hyphens (-). Start with a letter and end with a letter or digit. Minimum: 1 Maximum: 63
service_name	String	Service name. Start with a letter, and use only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
cluster_name	String	CCE cluster name.

Table 4-910 MicroServiceInfoNacosBase

Parameter	Type	Description
namespace	String	Namespace ID. If the default namespace public is used, leave this parameter empty. Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
cluster_name	String	Cluster name. The default value is DEFAULT . Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
group_name	String	Group name. The default value is DEFAULT_GROUP . Only letters, numbers, hyphens (-), underscores (_), periods (.), and colons (:) are allowed. Max.: 128 characters Minimum: 0 Maximum: 128
service_name	String	Microservice name. The value cannot start with @ or contain @@. Max.: 512 characters Minimum: 1 Maximum: 512
server_config	Array of NacosServerConfig objects	Nacos server configurations. Array Length: 1 - 9
user_info	NacosUserInfo object	Nacos user information.

Table 4-911 NacosServerConfig

Parameter	Type	Description
ip_address	String	IP address of the Nacos server. Minimum: 7 Maximum: 128

Parameter	Type	Description
port	Integer	Port number of the Nacos server. Range: 1–65535. Minimum: 1 Maximum: 65535
grpc_port	Integer	gRPC port number of the Nacos server. Default: port number + 1000 Range: 1–65535. Minimum: 1 Maximum: 65535

Table 4-912 NacosUserInfo

Parameter	Type	Description
user_name	String	Nacos username. Minimum: 1 Maximum: 64
password	String	Nacos password. Minimum: 1 Maximum: 64

Status code: 400**Table 4-913** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-914** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-915** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-916** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-917** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

- Updating a VPC channel of the server type

```
{
  "balance_strategy" : 2,
  "member_type" : "ip",
  "name" : "VPC_demo",
  "port" : 22,
  "type" : 2,
  "vpc_health_config" : {
    "http_code" : "200",
    "path" : "/vpc/demo",
    "port" : 22,
    "protocol" : "http",
    "threshold_abnormal" : 5,
    "threshold_normal" : 2,
    "time_interval" : 10,
    "timeout" : 5,
    "enable_client_ssl" : false
  },
  "member_groups" : [ {
    "member_group_name" : "test",
    "member_group_weight" : 1,
    "member_group_remark" : "remark"
  } ]
}
```

```
}, {  
  "member_group_name": "default",  
  "member_group_weight": 2,  
  "member_group_remark": "remark"  
}],  
"members": [ {  
  "host": "192.168.0.5",  
  "weight": 1,  
  "member_group_name": "test"  
}, {  
  "host": "192.168.1.124",  
  "weight": 2,  
  "member_group_name": "default"  
}]  
}
```

- Updating a VPC channel of the microservice type

```
{  
  "balance_strategy": 1,  
  "member_type": "ip",  
  "name": "VPC_demo",  
  "port": 22,  
  "type": 3,  
  "vpc_health_config": {  
    "http_code": "200",  
    "path": "/vpc/demo",  
    "port": 22,  
    "protocol": "http",  
    "threshold_abnormal": 5,  
    "threshold_normal": 2,  
    "time_interval": 10,  
    "timeout": 5,  
    "enable_client_ssl": false  
  },  
  "member_groups": [ {  
    "member_group_name": "test",  
    "member_group_weight": 1,  
    "member_group_remark": "remark",  
    "microservice_version": "v1",  
    "microservice_port": 80  
  }, {  
    "member_group_name": "default",  
    "member_group_weight": 2,  
    "member_group_remark": "remark",  
    "microservice_version": "v2",  
    "microservice_port": 80,  
    "microservice_labels": [ {  
      "label_name": "cluster_id",  
      "label_value": "c429700c-5dc4-482a-9c0e-99f6c0635113"  
    } ]  
  } ],  
  "members": [ {  
    "host": "192.168.0.5",  
    "weight": 1,  
    "member_group_name": "test"  
  }, {  
    "host": "192.168.1.124",  
    "weight": 2,  
    "member_group_name": "default"  
  } ],  
  "microservice_info": {  
    "service_type": "CCE",  
    "cce_info": {  
      "cluster_id": "ab1485b4f91b45abbcd560be591f7309",  
      "namespace": "default",  
      "workload_type": "deployment",  
      "app_name": "testapp"  
    }  
  }  
}
```

Example Responses

Status code: 200

OK

- Example 1

```
{
  "name": "VPC_demo",
  "port": 22,
  "balance_strategy": 2,
  "member_type": "ip",
  "dict_code": "",
  "create_time": "2020-07-23T07:11:57Z",
  "id": "18174f5f4f1a4dc29f33aeadd9788e5f",
  "status": 1,
  "member_groups": [ {
    "member_group_id": "c1ce135c705c4066853a0460b318fe16",
    "member_group_name": "test",
    "member_group_weight": 1,
    "member_group_remark": "remark",
    "create_time": "2020-07-23T07:11:57.244829604Z",
    "update_time": "2020-07-23T07:11:57.244829604Z"
  }, {
    "member_group_id": "c1ce135c705c4066853a0460b318fe17",
    "member_group_name": "default",
    "member_group_weight": 2,
    "member_group_remark": "remark",
    "create_time": "2020-07-23T07:11:57.244829604Z",
    "update_time": "2020-07-23T07:11:57.244829604Z"
  } ],
  "type": 2,
  "microservice_info": {
    "id": "",
    "instance_id": "",
    "service_type": "",
    "cse_info": {
      "cse_app_id": "",
      "engine_id": "",
      "engine_name": "",
      "register_address": "",
      "service_id": "",
      "service_name": ""
    },
    "cce_info": {
      "cluster_id": "",
      "cluster_name": "",
      "namespace": "",
      "workload_type": "",
      "app_name": ""
    },
    "create_time": "",
    "update_time": ""
  }
}
```

- Example 2

```
{
  "name": "VPC_demo",
  "id": "105c6902457144a4820dff8b1ad63331",
  "balance_strategy": 1,
  "dict_code": "",
  "create_time": "2020-07-23T07:11:57.244829604Z",
  "member_type": "ip",
  "port": 22,
  "status": 1,
  "member_groups": [ {
    "member_group_id": "c1ce135c705c4066853a0460b318fe16",
```

```
"member_group_name" : "test",
"member_group_weight" : 1,
"member_group_remark" : "remark",
"create_time" : "2020-07-23T07:11:57.244829604Z",
"update_time" : "2020-07-23T07:11:57.244829604Z",
"microservice_version" : "v1",
"microservice_port" : 80
}, {
  "member_group_id" : "c1ce135c705c4066853a0460b318fe17",
  "member_group_name" : "default",
  "member_group_weight" : 2,
  "member_group_remark" : "remark",
  "create_time" : "2020-07-23T07:11:57.244829604Z",
  "update_time" : "2020-07-23T07:11:57.244829604Z",
  "microservice_version" : "v2",
  "microservice_port" : 80,
  "microservice_labels" : [ {
    "label_name" : "cluster_id",
    "label_value" : "c429700c-5dc4-482a-9c0e-99f6c0635113"
  } ]
}, {
  "type" : 3,
  "microservice_info" : {
    "id" : "9483afa235be45158a70c19ab817ac65",
    "instance_id" : "eddc4d25480b4cd6b512f270a1b8b341",
    "service_type" : "CCE",
    "cse_info" : {
      "cse_app_id" : "",
      "engine_id" : "",
      "engine_name" : "",
      "register_address" : "",
      "service_id" : "",
      "service_name" : ""
    },
    "cce_info" : {
      "cluster_id" : "ab1485b4f91b45abbcd560be591f7309",
      "cluster_name" : "cce-test",
      "namespace" : "default",
      "workload_type" : "deployment",
      "app_name" : "testapp"
    },
    "create_time" : "2020-07-23T07:11:57.244829604Z",
    "update_time" : "2020-07-23T07:11:57.244829604Z"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2001",
  "error_msg" : "The request parameters must be specified, parameter name:members"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
}
```

```
{
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3023",
  "error_msg": "The VPC channel does not exist,id:56a7d7358e1b42459c9d730d65b14e59"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.3 Deleting a VPC Channel

Function

This API is used to delete a VPC channel.

Calling Method

For details, see [Calling APIs](#).

URI

```
DELETE /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/
{vpc_channel_id}
```

Table 4-918 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
vpc_channel_id	Yes	String	VPC channel ID.

Request Parameters

Table 4-919 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-920 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-921 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-922** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-923** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-924** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2012",  
}
```

```
{
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3023",
  "error_msg" : "The VPC channel does not exist,id:56a7d7358e1b42459c9d730d65b14e59"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.4 Querying VPC Channel Details

Function

This API is used to query the details of a VPC channel.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}

Table 4-925 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
vpc_channel_id	Yes	String	VPC channel ID.

Request Parameters

Table 4-926 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-927 Response body parameters

Parameter	Type	Description
name	String	VPC channel name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
port	Integer	Host port of the VPC channel. Range: 1–65535.
balance_strategy	Integer	Distribution algorithm. • 1: Weighted round robin (WRR). • 2: Weighted least connections (WLC). • 3: Source hashing. • 4: URI hashing. Default: 1
member_type	String	Member type of the VPC channel. • ip • ecs Default: ecs
type	Integer	VPC channel type. The default type is server. • 2: Server type • 3: Microservice type If vpc_channel_type is empty, the load balance channel type is determined by the type field. If the value of type is not 3 or the value of microservice_info is empty, the load balance channel type is server by default. If the value of type is 3 and the value of microservice_info is not empty, the load balance channel type is microservice. When you modify a load balance channel, the channel type will remain unchanged. This field is to be discarded. Use the vpc_channel_type field to specify the load balance channel type. Default: 2

Parameter	Type	Description
vpc_channel_type	String	VPC channel type. • builtin: server type • microservice: microservice type • reference: reference load balance channel If vpc_channel_type is empty, the load balance channel type depends on the value of the type field. If vpc_channel_type is non-empty and type is non-empty or non-zero, an error occurs when they are specified. If vpc_channel_type is non-empty and type is empty or 0, the value of vpc_channel_type is used to specify the load balance channel type. When you modify a load balance channel, the channel type will remain unchanged.
dict_code	String	Dictionary code of the VPC channel. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). This parameter is currently not supported. Minimum: 3 Maximum: 64
create_time	String	Time when the VPC channel is created.
id	String	VPC channel ID.
status	Integer	VPC channel status. • 1: normal • 2: abnormal
member_groups	Array of MemberGroupInfo objects	Backend server groups.
microservice_info	MicroServiceInfo object	Microservice information.
members	Array of VpcMemberInfo objects	Backend instances.
vpc_health_config	VpcHealthConfigInfo object	Health check details.

Table 4-928 MemberGroupInfo

Parameter	Type	Description
member_group_name	String	Name of the VPC channel's backend server group. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
member_groupRemark	String	Description of the backend server group. Maximum: 255
member_group_weight	Integer	Weight of the backend server group. If the server group contains servers and a weight has been set for it, the weight is automatically used to assign weights to servers in this group. Minimum: 0 Maximum: 100
dict_code	String	Dictionary code of the backend server group. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). Currently, this parameter is not supported. Minimum: 3 Maximum: 64
microservice_version	String	Version of the backend server group. This parameter is supported only when the VPC channel type is microservice. Maximum: 64
microservice_port	Integer	Port of the backend server group. This parameter is supported only when the VPC channel type is microservice. If the port number is 0, all addresses in the backend server group use the original load balancing port to inherit logic. Minimum: 0 Maximum: 65535
microservice_labels	Array of MicroserviceLabel objects	Tags of the backend server group. This parameter is supported only when the VPC channel type is microservice.

Parameter	Type	Description
reference_vpc_channel_id	String	ID of the reference load balance channel. This parameter is supported only when the VPC channel type is reference (vpc_channel_type=reference). Minimum: 0 Maximum: 64
member_group_id	String	ID of the backend server group of the VPC channel.
create_time	String	Time when the backend server group is created.
update_time	String	Time when the backend server group is updated.

Table 4-929 MicroserviceLabel

Parameter	Type	Description
label_name	String	Tag name. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63
label_value	String	Tag value. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Table 4-930 MicroServiceInfo

Parameter	Type	Description
id	String	Microservice ID.
instance_id	String	Gateway ID.

Parameter	Type	Description
service_type	String	Microservice type. • CSE: CSE microservice registration center. • CCE: CCE workload • CCE_SERVICE: CCE Service (not supported currently) • NACOS: Nacos engine. nacos_info is mandatory.
cse_info	MicroServiceInfoCSE object	CSE microservice details.
cce_info	MicroServiceInfoCCE object	CCE microservice workload details.
cce_service_info	MicroServiceInfoCCEService object	CCE microservice Service details.
nacos_info	MicroServiceInfoNacosBase object	Nacos basic information.
update_time	String	Microservice update time.
create_time	String	Microservice creation time.

Table 4-931 MicroServiceInfoCSE

Parameter	Type	Description
engine_id	String	Microservice engine ID. Maximum: 64
service_id	String	Microservice ID. Maximum: 64
engine_name	String	Microservice engine name.
service_name	String	Microservice name.
register_address	String	Registration center address.
cse_app_id	String	App to which the microservice belongs.
version	String	Microservice version, which has been discarded and is reflected in the version of the backend server group. Maximum: 64

Table 4-932 MicroServiceInfoCCE

Parameter	Type	Description
cluster_id	String	CCE cluster ID. Maximum: 64
namespace	String	Namespace. Maximum: 64
workload_type	String	Workload type. • deployment • statefulset • daemonset
app_name	String	App name. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
label_key	String	Service label key. Start with a letter or digit, and use only letters, digits, and these special characters: -_./:(). (1 to 64 characters) Minimum: 1 Maximum: 64
label_value	String	Service label value. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
cluster_name	String	CCE cluster name.

Table 4-933 MicroServiceInfoCCEService

Parameter	Type	Description
cluster_id	String	CCE cluster ID. Maximum: 64

Parameter	Type	Description
namespace	String	Namespace. 1 to 63 characters. Use lowercase letters, digits, and hyphens (-). Start with a letter and end with a letter or digit. Minimum: 1 Maximum: 63
service_name	String	Service name. Start with a letter, and use only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
cluster_name	String	CCE cluster name.

Table 4-934 MicroServiceInfoNacosBase

Parameter	Type	Description
namespace	String	Namespace ID. If the default namespace public is used, leave this parameter empty. Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
cluster_name	String	Cluster name. The default value is DEFAULT . Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
group_name	String	Group name. The default value is DEFAULT_GROUP . Only letters, numbers, hyphens (-), underscores (_), periods (.), and colons (:) are allowed. Max.: 128 characters Minimum: 0 Maximum: 128

Parameter	Type	Description
service_name	String	Microservice name. The value cannot start with @ or contain @@. Max.: 512 characters Minimum: 1 Maximum: 512
server_config	Array of NacosServerConfig objects	Nacos server configurations. Array Length: 1 - 9
user_info	NacosUserInfo object	Nacos user information.

Table 4-935 NacosServerConfig

Parameter	Type	Description
ip_address	String	IP address of the Nacos server. Minimum: 7 Maximum: 128
port	Integer	Port number of the Nacos server. Range: 1-65535. Minimum: 1 Maximum: 65535
grpc_port	Integer	gRPC port number of the Nacos server. Default: port number + 1000 Range: 1-65535. Minimum: 1 Maximum: 65535

Table 4-936 NacosUserInfo

Parameter	Type	Description
user_name	String	Nacos username. Minimum: 1 Maximum: 64
password	String	Nacos password. Minimum: 1 Maximum: 64

Table 4-937 VpcMemberInfo

Parameter	Type	Description
host	String	Backend server address. This parameter is required when the member type is IP address. Maximum: 255
weight	Integer	Weight. The higher the weight is, the more requests a backend service will receive. Minimum: 0 Maximum: 10000
is_backup	Boolean	Indicates whether the backend service is a standby node. After you enable this option, the corresponding backend service serves as the standby node and works only when all non-standby nodes are faulty. This function is supported only when your gateway has been upgraded to the corresponding version. If your gateway does not support this function, contact technical support. Default: false
member_group_name	String	Backend server group name. The server group facilitates backend service address modification.
status	Integer	Backend server status. 1: available 2: unavailable
port	Integer	Backend server port. Minimum: 0 Maximum: 65535
ecs_id	String	Backend server ID. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), and underscores (_). Maximum: 255

Parameter	Type	Description
ecs_name	String	Backend server name. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), underscores (_), and periods (.). Maximum: 64
id	String	Backend instance ID.
vpc_channel_id	String	VPC channel ID.
create_time	String	Time when the backend server is added to the VPC channel.
member_group_id	String	Backend server group ID.
health_status	String	Health status of the backend instance of the load balance channel. The value can be unknown, healthy, or unhealthy, indicating that no health check is performed, healthy, or unhealthy, respectively.

Table 4-938 VpcHealthConfigInfo

Parameter	Type	Description
protocol	String	Protocol for performing health checks on backend servers in the VPC channel. • TCP • HTTP • HTTPS
path	String	Destination path for health checks. This parameter is required if protocol is set to http or https.
method	String	Request method for health checks. Default: GET

Parameter	Type	Description
port	Integer	Destination port for health checks. If this parameter is not specified or set to 0, the host port of the VPC channel is used. If this parameter is set to a non-zero value, the corresponding port is used for health checks. Minimum: 0 Maximum: 65535
threshold_normal	Integer	Healthy threshold. It refers to the number of consecutive successful checks required for a backend server to be considered healthy. Minimum: 1 Maximum: 10
threshold_abnormal	Integer	Unhealthy threshold, which refers to the number of consecutive failed checks required for a backend server to be considered unhealthy. Minimum: 1 Maximum: 10
time_interval	Integer	Interval between consecutive checks. Unit: s. The value must be greater than the value of timeout. Minimum: 1 Maximum: 300
http_code	String	Response codes for determining a successful HTTP response. The value can be any integer within 100–599 in one of the following formats: • Multiple values, for example, 200,201,202 • Range, for example, 200-299 • Multiple values and ranges, for example, 201,202,210-299. This parameter is required if protocol is set to http.

Parameter	Type	Description
enable_client_ssl	Boolean	Indicates whether to enable two-way authentication. If this function is enabled, the certificate specified in the backend_client_certificate configuration item of the instance is used. Default: false
status	Integer	Health check result. • 1: available • 2: unavailable
timeout	Integer	Timeout for determining whether a health check fails. Unit: s. The value must be less than the value of time_interval. Minimum: 1 Maximum: 30
vpc_channel_id	String	VPC channel ID.
id	String	Health check ID.
create_time	String	Creation time.

Status code: 400**Table 4-939** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-940** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-941 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-942** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-943** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

- Example 1

```
{
  "name": "VPC_demo",
  "port": 22,
  "balance_strategy": 1,
  "member_type": "ip",
  "dict_code": "",
  "create_time": "2020-07-23T07:11:57.244829604Z",
  "id": "56a7d7358e1b42459c9d730d65b14e59",
  "status": 1,
  "member_groups": [ ],
  "type": 2,
  "members": [ {
    "host": "192.168.0.5",
    "weight": 1,
```



```
"is_backup" : false,
"member_group_name" : "",
"status" : 1,
"port" : 22,
"ecs_id" : "192.168.0.5",
"ecs_name" : "192.168.0.5",
"id" : "be63c6260a1043888187f84af39c9f0e",
"vpc_channel_id" : "56a7d7358e1b42459c9d730d65b14e59",
"create_time" : "2020-07-23T07:11:57Z",
"member_group_id" : "",
"health_status" : "healthy"
}, {
  "host" : "192.168.1.124",
  "weight" : 2,
  "is_backup" : false,
  "member_group_name" : "",
  "status" : 1,
  "port" : 22,
  "ecs_id" : "192.168.1.124",
  "ecs_name" : "192.168.1.124",
  "id" : "a57b13f1b89b417ca8acd76909e6df67",
  "vpc_channel_id" : "56a7d7358e1b42459c9d730d65b14e59",
  "create_time" : "2020-07-23T07:11:57Z",
  "member_group_id" : "",
  "health_status" : "unhealthy"
} ],
"vpc_health_config" : {
  "protocol" : "http",
  "path" : "/vpc/demo",
  "method" : "GET",
  "port" : 22,
  "threshold_normal" : 2,
  "threshold_abnormal" : 5,
  "time_interval" : 10,
  "http_code" : "200",
  "enable_client_ssl" : false,
  "status" : 1,
  "timeout" : 5,
  "vpc_channel_id" : "56a7d7358e1b42459c9d730d65b14e59",
  "id" : "3b3d02026c5f402d85e8645ea95b0816",
  "create_time" : "2020-07-23T07:11:57Z"
},
"microservice_info" : {
  "id" : "",
  "instance_id" : "",
  "service_type" : "",
  "cse_info" : {
    "cse_app_id" : "",
    "engine_id" : "",
    "engine_name" : "",
    "register_address" : "",
    "service_id" : "",
    "service_name" : ""
  },
  "cce_info" : {
    "cluster_id" : "",
    "cluster_name" : "",
    "namespace" : "",
    "workload_type" : "",
    "app_name" : ""
  },
  "create_time" : "",
  "update_time" : ""
}
}
```

- Example 2

```
{
  "name" : "VPC_demo",
  "id" : "105c6902457144a4820dff8b1ad63331",
```

```
"balance_strategy" : 1,
"dict_code" : "",
"create_time" : "2020-07-23T07:11:57.244829604Z",
"member_type" : "ip",
"port" : 22,
"status" : 1,
"member_groups" : [ {
  "member_group_id" : "c1ce135c705c4066853a0460b318fe16",
  "member_group_name" : "test",
  "member_group_weight" : 1,
  "member_group_remark" : "remark",
  "create_time" : "2020-07-23T07:11:57.244829604Z",
  "update_time" : "2020-07-23T07:11:57.244829604Z",
  "microservice_version" : "v1",
  "microservice_port" : 80
}, {
  "member_group_id" : "c1ce135c705c4066853a0460b318fe17",
  "member_group_name" : "default",
  "member_group_weight" : 2,
  "member_group_remark" : "remark",
  "create_time" : "2020-07-23T07:11:57.244829604Z",
  "update_time" : "2020-07-23T07:11:57.244829604Z",
  "microservice_version" : "v2",
  "microservice_port" : 80
} ],
"type" : 3,
"vpc_health_config" : {
  "protocol" : "http",
  "path" : "/vpc/demo",
  "method" : "GET",
  "port" : 22,
  "threshold_normal" : 2,
  "threshold_abnormal" : 5,
  "time_interval" : 10,
  "http_code" : "200",
  "enable_client_ssl" : false,
  "status" : 1,
  "timeout" : 5,
  "vpc_channel_id" : "56a7d7358e1b42459c9d730d65b14e59",
  "id" : "3b3d02026c5f402d85e8645ea95b0816",
  "create_time" : "2020-07-23T07:11:57Z"
},
"microservice_info" : {
  "id" : "9483afa235be45158a70c19ab817ac65",
  "instance_id" : "eddc4d25480b4cd6b512f270a1b8b341",
  "service_type" : "CCE",
  "cse_info" : {
    "cse_app_id" : "",
    "engine_id" : "",
    "engine_name" : "",
    "register_address" : "",
    "service_id" : "",
    "service_name" : ""
  },
  "cce_info" : {
    "cluster_id" : "ab1485b4f91b45abbcd560be591f7309",
    "cluster_name" : "cce-test",
    "namespace" : "default",
    "workload_type" : "deployment",
    "app_name" : "testapp"
  },
  "create_time" : "2020-07-23T07:11:57.244829604Z",
  "update_time" : "2020-07-23T07:11:57.244829604Z"
}
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3023",
  "error_msg" : "The VPC channel does not exist,id:56a7d7358e1b42459c9d730d65b14e59"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.5 Querying VPC Channels

Function

This API is used to query the VPC channels under a gateway.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels

Table 4-944 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-945 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
id	No	String	VPC channel ID.

Parameter	Mandatory	Type	Description
name	No	String	VPC channel name.
dict_code	No	String	Dictionary code of the VPC channel. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). This parameter is currently not supported. Minimum: 3 Maximum: 64
precise_search	No	String	Parameter name for exact matching. Separate multiple parameter names with commas (,). Currently, name and member_group_name are supported.
member_host	No	String	Backend service address. By default, exact match is used. Fuzzy match is not supported.
member_port	No	Integer	Backend server port. Minimum: 0 Maximum: 65535
member_group_name	No	String	Backend server group name.
member_group_id	No	String	Backend server group ID.
vpc_channel_type	No	String	VPC channel type. • builtin: server type • microservice: microservice type • reference: reference load balance channel

Request Parameters

Table 4-946 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-947 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
vpc_channels	Array of VpcChannelInfo objects	VPC channel list.

Table 4-948 VpcChannelInfo

Parameter	Type	Description
name	String	VPC channel name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
port	Integer	Host port of the VPC channel. Range: 1-65535.

Parameter	Type	Description
balance_strategy	Integer	Distribution algorithm. • 1: Weighted round robin (WRR). • 2: Weighted least connections (WLC). • 3: Source hashing. • 4: URI hashing. Default: 1
member_type	String	Member type of the VPC channel. • ip • ecs Default: ecs
type	Integer	VPC channel type. The default type is server. • 2: Server type • 3: Microservice type If vpc_channel_type is empty, the load balance channel type is determined by the type field. If the value of type is not 3 or the value of microservice_info is empty, the load balance channel type is server by default. If the value of type is 3 and the value of microservice_info is not empty, the load balance channel type is microservice. When you modify a load balance channel, the channel type will remain unchanged. This field is to be discarded. Use the vpc_channel_type field to specify the load balance channel type. Default: 2

Parameter	Type	Description
vpc_channel_type	String	VPC channel type. • builtin: server type • microservice: microservice type • reference: reference load balance channel If vpc_channel_type is empty, the load balance channel type depends on the value of the type field. If vpc_channel_type is non-empty and type is non-empty or non-zero, an error occurs when they are specified. If vpc_channel_type is non-empty and type is empty or 0, the value of vpc_channel_type is used to specify the load balance channel type. When you modify a load balance channel, the channel type will remain unchanged.
dict_code	String	Dictionary code of the VPC channel. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). This parameter is currently not supported. Minimum: 3 Maximum: 64
create_time	String	Time when the VPC channel is created.
id	String	VPC channel ID.
status	Integer	VPC channel status. • 1: normal • 2: abnormal
member_groups	Array of MemberGroupInfo objects	Backend server groups.
microservice_info	MicroServiceInfo object	Microservice information.

Table 4-949 MemberGroupInfo

Parameter	Type	Description
member_group_name	String	Name of the VPC channel's backend server group. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
member_group_remark	String	Description of the backend server group. Maximum: 255
member_group_weight	Integer	Weight of the backend server group. If the server group contains servers and a weight has been set for it, the weight is automatically used to assign weights to servers in this group. Minimum: 0 Maximum: 100
dict_code	String	Dictionary code of the backend server group. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). Currently, this parameter is not supported. Minimum: 3 Maximum: 64
microservice_version	String	Version of the backend server group. This parameter is supported only when the VPC channel type is microservice. Maximum: 64
microservice_port	Integer	Port of the backend server group. This parameter is supported only when the VPC channel type is microservice. If the port number is 0, all addresses in the backend server group use the original load balancing port to inherit logic. Minimum: 0 Maximum: 65535
microservice_labels	Array of MicroserviceLabel objects	Tags of the backend server group. This parameter is supported only when the VPC channel type is microservice.

Parameter	Type	Description
reference_vpc_channel_id	String	ID of the reference load balance channel. This parameter is supported only when the VPC channel type is reference (vpc_channel_type=reference). Minimum: 0 Maximum: 64
member_group_id	String	ID of the backend server group of the VPC channel.
create_time	String	Time when the backend server group is created.
update_time	String	Time when the backend server group is updated.

Table 4-950 MicroserviceLabel

Parameter	Type	Description
label_name	String	Tag name. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63
label_value	String	Tag value. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Table 4-951 MicroServiceInfo

Parameter	Type	Description
id	String	Microservice ID.
instance_id	String	Gateway ID.

Parameter	Type	Description
service_type	String	Microservice type. • CSE: CSE microservice registration center. • CCE: CCE workload • CCE_SERVICE: CCE Service (not supported currently) • NACOS: Nacos engine. nacos_info is mandatory.
cse_info	MicroServiceInfoCSE object	CSE microservice details.
cce_info	MicroServiceInfoCCE object	CCE microservice workload details.
cce_service_info	MicroServiceInfoCCEService object	CCE microservice Service details.
nacos_info	MicroServiceInfoNacosBase object	Nacos basic information.
update_time	String	Microservice update time.
create_time	String	Microservice creation time.

Table 4-952 MicroServiceInfoCSE

Parameter	Type	Description
engine_id	String	Microservice engine ID. Maximum: 64
service_id	String	Microservice ID. Maximum: 64
engine_name	String	Microservice engine name.
service_name	String	Microservice name.
register_address	String	Registration center address.
cse_app_id	String	App to which the microservice belongs.
version	String	Microservice version, which has been discarded and is reflected in the version of the backend server group. Maximum: 64

Table 4-953 MicroServiceInfoCCE

Parameter	Type	Description
cluster_id	String	CCE cluster ID. Maximum: 64
namespace	String	Namespace. Maximum: 64
workload_type	String	Workload type. • deployment • statefulset • daemonset
app_name	String	App name. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
label_key	String	Service label key. Start with a letter or digit, and use only letters, digits, and these special characters: -_./:(). (1 to 64 characters) Minimum: 1 Maximum: 64
label_value	String	Service label value. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
cluster_name	String	CCE cluster name.

Table 4-954 MicroServiceInfoCCEService

Parameter	Type	Description
cluster_id	String	CCE cluster ID. Maximum: 64

Parameter	Type	Description
namespace	String	Namespace. 1 to 63 characters. Use lowercase letters, digits, and hyphens (-). Start with a letter and end with a letter or digit. Minimum: 1 Maximum: 63
service_name	String	Service name. Start with a letter, and use only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
cluster_name	String	CCE cluster name.

Table 4-955 MicroServiceInfoNacosBase

Parameter	Type	Description
namespace	String	Namespace ID. If the default namespace public is used, leave this parameter empty. Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
cluster_name	String	Cluster name. The default value is DEFAULT . Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
group_name	String	Group name. The default value is DEFAULT_GROUP . Only letters, numbers, hyphens (-), underscores (_), periods (.), and colons (:) are allowed. Max.: 128 characters Minimum: 0 Maximum: 128

Parameter	Type	Description
service_name	String	Microservice name. The value cannot start with @ or contain @@. Max.: 512 characters Minimum: 1 Maximum: 512
server_config	Array of NacosServerConfig objects	Nacos server configurations. Array Length: 1 - 9
user_info	NacosUserInfo object	Nacos user information.

Table 4-956 NacosServerConfig

Parameter	Type	Description
ip_address	String	IP address of the Nacos server. Minimum: 7 Maximum: 128
port	Integer	Port number of the Nacos server. Range: 1-65535. Minimum: 1 Maximum: 65535
grpc_port	Integer	gRPC port number of the Nacos server. Default: port number + 1000 Range: 1-65535. Minimum: 1 Maximum: 65535

Table 4-957 NacosUserInfo

Parameter	Type	Description
user_name	String	Nacos username. Minimum: 1 Maximum: 64
password	String	Nacos password. Minimum: 1 Maximum: 64

Status code: 400**Table 4-958** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-959** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-960** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-961** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-962** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total": 2,
  "size": 2,
  "vpc_channels": [ {
    "name": "channel 1",
    "port": 8080,
    "balance_strategy": 1,
    "member_type": "ip",
    "dict_code": "",
    "create_time": "2020-07-23T07:24:33Z",
    "id": "105c6902457144a4820dff8b1ad63331",
    "status": 1,
    "member_groups": [ ],
    "type": 2,
    "microservice_info": {
      "id": "",
      "instance_id": "",
      "service_type": "",
      "cse_info": {
        "cse_app_id": "",
        "engine_id": "",
        "engine_name": "",
        "register_address": "",
        "service_id": "",
        "service_name": ""
      },
      "cce_info": {
        "cluster_id": "",
        "cluster_name": "",
        "namespace": "",
        "workload_type": "",
        "app_name": ""
      },
      "create_time": "",
      "update_time": ""
    }
  }, {
    "name": "channel 2",
    "port": 8088,
    "balance_strategy": 2,
    "member_type": "ip",
    "dict_code": "",
    "create_time": "2020-07-23T07:11:57Z",
    "id": "56a7d7358e1b42459c9d730d65b14e59",
    "status": 1,
    "member_groups": [ ],
    "type": 3,
    "microservice_info": {
      "id": "9483afa235be45158a70c19ab817ac65",
      "instance_id": "eddc4d25480b4cd6b512f270a1b8b341",
```



```
{
  "service_type": "CCE",
  "cse_info": {
    "cse_app_id": "",
    "engine_id": "",
    "engine_name": "",
    "register_address": "",
    "service_id": "",
    "service_name": ""
  },
  "cce_info": {
    "cluster_id": "ab1485b4f91b45abbcd560be591f7309",
    "cluster_name": "cce-test",
    "namespace": "default",
    "workload_type": "deployment",
    "app_name": "testapp"
  },
  "create_time": "2020-07-23T07:11:57.244829604Z",
  "update_time": "2020-07-23T07:11:57.244829604Z"
}
}]
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2011",
  "error_msg": "The request parameters must be specified,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3030",
  "error_msg": "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.6 Adding or Updating Backend Instances

Function

This API is used to add backend instances to a VPC channel.

If a backend instance with the specified address already exists, the instance information is updated. If the request body contains multiple backend instance definitions with the same address, the first definition is used.

Backend instances cannot be added or updated for a reference load balance channel.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members

Table 4-963 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
vpc_channel_id	Yes	String	VPC channel ID.

Request Parameters

Table 4-964 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-965 Request body parameters

Parameter	Mandatory	Type	Description
members	Yes	Array of MemberInfo objects	Backend instances.

Table 4-966 MemberInfo

Parameter	Mandatory	Type	Description
host	No	String	Backend server address. This parameter is required when the member type is IP address. Maximum: 255
weight	No	Integer	Weight. The higher the weight is, the more requests a backend service will receive. Minimum: 0 Maximum: 10000

Parameter	Mandatory	Type	Description
is_backup	No	Boolean	Indicates whether the backend service is a standby node. After you enable this option, the corresponding backend service serves as the standby node and works only when all non-standby nodes are faulty. This function is supported only when your gateway has been upgraded to the corresponding version. If your gateway does not support this function, contact technical support. Default: false
member_group_name	No	String	Backend server group name. The server group facilitates backend service address modification.
status	No	Integer	Backend server status. • 1: available • 2: unavailable
port	No	Integer	Backend server port. Minimum: 0 Maximum: 65535
ecs_id	No	String	Backend server ID. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), and underscores (_). Maximum: 255
ecs_name	No	String	Backend server name. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), underscores (_), and periods (.). Maximum: 64

Response Parameters

Status code: 201

Table 4-967 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
members	Array of VpcMemberInfo objects	Cloud server list.

Table 4-968 VpcMemberInfo

Parameter	Type	Description
host	String	Backend server address. This parameter is required when the member type is IP address. Maximum: 255
weight	Integer	Weight. The higher the weight is, the more requests a backend service will receive. Minimum: 0 Maximum: 10000
is_backup	Boolean	Indicates whether the backend service is a standby node. After you enable this option, the corresponding backend service serves as the standby node and works only when all non-standby nodes are faulty. This function is supported only when your gateway has been upgraded to the corresponding version. If your gateway does not support this function, contact technical support. Default: false
member_group_name	String	Backend server group name. The server group facilitates backend service address modification.

Parameter	Type	Description
status	Integer	Backend server status. 1: available 2: unavailable
port	Integer	Backend server port. Minimum: 0 Maximum: 65535
ecs_id	String	Backend server ID. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), and underscores (_). Maximum: 255
ecs_name	String	Backend server name. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), underscores (_), and periods (.). Maximum: 64
id	String	Backend instance ID.
vpc_channel_id	String	VPC channel ID.
create_time	String	Time when the backend server is added to the VPC channel.
member_group_id	String	Backend server group ID.
health_status	String	Health status of the backend instance of the load balance channel. The value can be unknown, healthy, or unhealthy, indicating that no health check is performed, healthy, or unhealthy, respectively.

Status code: 400

Table 4-969 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-970** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-971** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-972** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-973** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

- Adding a cloud server IP address to a VPC channel

```
{  
  "members" : [ {
```

```
"host" : "192.168.2.25",
"weight" : 1,
"member_group_name" : "test"
}]
}
```

- Adding a cloud server name to a VPC channel

```
{
  "members" : [ {
    "ecs_id" : "1082720c-3c15-409c-9ae3-4983ddfb6a9d",
    "ecs_name" : "APIGtest02",
    "weight" : 2
  } ]
}
```

Example Responses

Status code: 201

Created

- Example 1

```
{
  "total" : 1,
  "size" : 1,
  "members" : [ {
    "host" : "192.168.2.25",
    "weight" : 1,
    "is_backup" : false,
    "member_group_name" : "test",
    "status" : 1,
    "port" : 22,
    "ecs_id" : "3082720c-3c15-409c-9ae3-4983ddfb6a9d",
    "ecs_name" : "APIGtest",
    "id" : "683b6807cad54122a6777ad047a6178e",
    "vpc_channel_id" : "105c6902457144a4820dff8b1ad63331",
    "create_time" : "2020-07-23T09:13:24Z",
    "member_group_id" : "cf868f0224084710a1e188b7d3057c52"
  } ]
}
```

- Example 2

```
{
  "total" : 2,
  "size" : 2,
  "members" : [ {
    "host" : "192.168.0.17",
    "weight" : 2,
    "is_backup" : false,
    "member_group_name" : "test02",
    "status" : 1,
    "port" : 22,
    "ecs_id" : "1082720c-3c15-409c-9ae3-4983ddfb6a9d",
    "ecs_name" : "APIGtest02",
    "id" : "5c868f0224084710a1e188b7d3057c52",
    "vpc_channel_id" : "105c6902457144a4820dff8b1ad63331",
    "create_time" : "2020-07-23T09:03:53Z",
    "member_group_id" : "df868f0224084710a1e188b7d3057c52",
    "health_status" : "unhealthy"
  }, {
    "host" : "192.168.0.39",
    "weight" : 1,
    "is_backup" : false,
    "member_group_name" : "test01",
    "status" : 1,
    "port" : 22,
    "ecs_id" : "e1e1104f-1254-4ac6-8ed7-366bec84f36e",
    "ecs_name" : "APIGtest01",
  } ]
}
```



```
{
  "id" : "33ac0e39d005492eb1f4683e66d1a0d1",
  "vpc_channel_id" : "105c6902457144a4820dff8b1ad63331",
  "create_time" : "2020-07-23T07:24:34Z",
  "member_group_id" : "ef868f0224084710a1e188b7d3057c42",
  "health_status" : "unhealthy"
}]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2004",
  "error_msg" : "The parameter value is outside the allowable range,parameterName:weight. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3023",
  "error_msg" : "The VPC channel does not exist,id:56a7d7358e1b42459c9d730d65b14e59"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.7 Querying Backend Servers of a VPC Channel

Function

This API is used to query the backend instances of a specified VPC channel.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members

Table 4-974 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
vpc_channel_id	Yes	String	VPC channel ID.

Table 4-975 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
name	No	String	Cloud server name.
member_group_name	No	String	Backend server group name.
member_group_id	No	String	Backend server group ID.
precise_search	No	String	Parameter name for exact matching. Separate multiple parameter names with commas (,). Currently, name and member_group_name are supported.

Request Parameters

Table 4-976 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-977 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
members	Array of VpcMemberInfo objects	Cloud server list.

Table 4-978 VpcMemberInfo

Parameter	Type	Description
host	String	Backend server address. This parameter is required when the member type is IP address. Maximum: 255
weight	Integer	Weight. The higher the weight is, the more requests a backend service will receive. Minimum: 0 Maximum: 10000
is_backup	Boolean	Indicates whether the backend service is a standby node. After you enable this option, the corresponding backend service serves as the standby node and works only when all non-standby nodes are faulty. This function is supported only when your gateway has been upgraded to the corresponding version. If your gateway does not support this function, contact technical support. Default: false
member_group_name	String	Backend server group name. The server group facilitates backend service address modification.

Parameter	Type	Description
status	Integer	Backend server status. 1: available 2: unavailable
port	Integer	Backend server port. Minimum: 0 Maximum: 65535
ecs_id	String	Backend server ID. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), and underscores (_). Maximum: 255
ecs_name	String	Backend server name. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), underscores (_), and periods (.). Maximum: 64
id	String	Backend instance ID.
vpc_channel_id	String	VPC channel ID.
create_time	String	Time when the backend server is added to the VPC channel.
member_group_id	String	Backend server group ID.
health_status	String	Health status of the backend instance of the load balance channel. The value can be unknown, healthy, or unhealthy, indicating that no health check is performed, healthy, or unhealthy, respectively.

Status code: 400

Table 4-979 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-980** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-981** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-982** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-983** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total": 2,
  "size": 2,
  "members": [ {
    "host": "192.168.0.5",
    "weight": 1,
    "is_backup": false,
    "member_group_name": "",
    "status": 1,
    "port": 22,
    "ecs_id": "192.168.0.5",
    "ecs_name": "192.168.0.5",
    "id": "be63c6260a1043888187f84af39c9f0e",
    "vpc_channel_id": "56a7d7358e1b42459c9d730d65b14e59",
    "create_time": "2020-07-23T07:11:57Z",
    "member_group_id": "",
    "health_status": "unhealthy"
  }, {
    "host": "192.168.1.124",
    "weight": 2,
    "is_backup": false,
    "member_group_name": "",
    "status": 1,
    "port": 22,
    "ecs_id": "192.168.1.124",
    "ecs_name": "192.168.1.124",
    "id": "a57b13f1b89b417ca8acd76909e6df67",
    "vpc_channel_id": "56a7d7358e1b42459c9d730d65b14e59",
    "create_time": "2020-07-23T07:11:57Z",
    "member_group_id": "",
    "health_status": "unhealthy"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2012",
  "error_msg": "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3023",
  "error_msg" : "The VPC channel does not exist,id:56a7d7358e1b42459c9d730d65b14e59"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.8 Updating Backend Instances

Function

This API is used to update the backend instances of a specified VPC channel. During the update, the request parameters overwrite the backend instances of the corresponding cloud server group. If no cloud server group is specified, all cloud server groups are overwritten.

Backend instances cannot be updated for a reference load balance channel.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members

Table 4-984 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
vpc_channel_id	Yes	String	VPC channel ID.

Request Parameters

Table 4-985 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-986 Request body parameters

Parameter	Mandatory	Type	Description
members	No	Array of MemberInfo objects	Backend instances.

Parameter	Mandatory	Type	Description
member_group_name	No	String	Backend server group to be modified. If this parameter is not specified, all backends defined by members for the VPC channel are modified. If this parameter is specified, only the backend instances in the backend server group defined by members are modified. Input parameters of other backend server groups are ignored. For example, if member_group_name=primary is passed, only backend instances of backend server group 105c6902457144a4820dff8b1ad63331 in members are modified.

Table 4-987 MemberInfo

Parameter	Mandatory	Type	Description
host	No	String	Backend server address. This parameter is required when the member type is IP address. Maximum: 255
weight	No	Integer	Weight. The higher the weight is, the more requests a backend service will receive. Minimum: 0 Maximum: 10000

Parameter	Mandatory	Type	Description
is_backup	No	Boolean	Indicates whether the backend service is a standby node. After you enable this option, the corresponding backend service serves as the standby node and works only when all non-standby nodes are faulty. This function is supported only when your gateway has been upgraded to the corresponding version. If your gateway does not support this function, contact technical support. Default: false
member_group_name	No	String	Backend server group name. The server group facilitates backend service address modification.
status	No	Integer	Backend server status. • 1: available • 2: unavailable
port	No	Integer	Backend server port. Minimum: 0 Maximum: 65535
ecs_id	No	String	Backend server ID. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), and underscores (_). Maximum: 255
ecs_name	No	String	Backend server name. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), underscores (_), and periods (.). Maximum: 64

Response Parameters

Status code: 200

Table 4-988 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
members	Array of VpcMemberInfo objects	Cloud server list.

Table 4-989 VpcMemberInfo

Parameter	Type	Description
host	String	Backend server address. This parameter is required when the member type is IP address. Maximum: 255
weight	Integer	Weight. The higher the weight is, the more requests a backend service will receive. Minimum: 0 Maximum: 10000
is_backup	Boolean	Indicates whether the backend service is a standby node. After you enable this option, the corresponding backend service serves as the standby node and works only when all non-standby nodes are faulty. This function is supported only when your gateway has been upgraded to the corresponding version. If your gateway does not support this function, contact technical support. Default: false
member_group_name	String	Backend server group name. The server group facilitates backend service address modification.

Parameter	Type	Description
status	Integer	Backend server status. 1: available 2: unavailable
port	Integer	Backend server port. Minimum: 0 Maximum: 65535
ecs_id	String	Backend server ID. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), and underscores (_). Maximum: 255
ecs_name	String	Backend server name. This parameter is required if the backend instance type is ecs. The value can contain 1 to 64 characters, including letters, digits, hyphens (-), underscores (_), and periods (.). Maximum: 64
id	String	Backend instance ID.
vpc_channel_id	String	VPC channel ID.
create_time	String	Time when the backend server is added to the VPC channel.
member_group_id	String	Backend server group ID.
health_status	String	Health status of the backend instance of the load balance channel. The value can be unknown, healthy, or unhealthy, indicating that no health check is performed, healthy, or unhealthy, respectively.

Status code: 400

Table 4-990 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-991** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-992** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-993** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-994** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

- Updating non-standby backend instances of a VPC channel

```
{  
  "member_group_name": "primary",  
}
```

```
"members" : [ {  
  "host" : "192.168.2.25",  
  "weight" : 1,  
  "is_backup" : false,  
  "member_group_name" : "primary"  
} ]  
}
```

- Updating all backend instances of a VPC channel

```
{  
  "members" : [ {  
    "ecs_id" : "1082720c-3c15-409c-9ae3-4983ddfb6a9d",  
    "ecs_name" : "APIGtest02",  
    "weight" : 2  
  } ]  
}
```

Example Responses

Status code: 200

OK

- Example 1

```
{  
  "total" : 1,  
  "size" : 1,  
  "members" : [ {  
    "host" : "192.168.2.25",  
    "weight" : 1,  
    "is_backup" : false,  
    "member_group_name" : "primary",  
    "port" : 22,  
    "status" : 1,  
    "ecs_id" : "192.168.2.25",  
    "ecs_name" : "192.168.2.25",  
    "id" : "683b6807cad54122a6777ad047a6178e",  
    "vpc_channel_id" : "56a7d7358e1b42459c9d730d65b14e59",  
    "create_time" : "2020-07-23T09:13:24Z",  
    "member_group_id" : "631b551cddda40478ef720163a9412ed"  
  } ]  
}
```

- Example 2

```
{  
  "total" : 1,  
  "size" : 1,  
  "members" : [ {  
    "host" : "192.168.0.17",  
    "weight" : 2,  
    "is_backup" : false,  
    "member_group_name" : "primary",  
    "port" : 22,  
    "status" : 1,  
    "ecs_id" : "1082720c-3c15-409c-9ae3-4983ddfb6a9d",  
    "ecs_name" : "APIGtest02",  
    "id" : "5c868f0224084710a1e188b7d3057c52",  
    "vpc_channel_id" : "105c6902457144a4820dff8b1ad63331",  
    "create_time" : "2020-07-23T09:03:53Z",  
    "member_group_id" : "631b551cddda40478ef720163a9412ed"  
  } ]  
}
```

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2001",  
}
```

```
{
  "error_msg" : "The request parameters must be specified, parameter name:members"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3023",
  "error_msg" : "The VPC channel does not exist,id:56a7d7358e1b42459c9d730d65b14e59"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.9 Removing a Backend Server

Function

This API is used to delete a backend instance from a specified VPC channel.

Backend instances cannot be deleted for a reference load balance channel.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/
{vpc_channel_id}/members/{member_id}

Table 4-995 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
vpc_channel_id	Yes	String	VPC channel ID.
member_id	Yes	String	Backend instance ID.

Request Parameters

Table 4-996 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400**Table 4-997** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-998** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-999** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1000** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1001 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3024",
  "error_msg" : "The VPC instance does not exist,id:be63c6260a1043888187f84af39c9f0e"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.10 Enabling Backend Servers

Function

This API is used to enable backend servers of a VPC channel.

The statuses of backend servers cannot be modified for a reference load balance channel.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/batch-enable

Table 4-1002 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Parameter	Mandatory	Type	Description
vpc_channel_id	Yes	String	VPC channel ID.

Request Parameters

Table 4-1003 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1004 Request body parameters

Parameter	Mandatory	Type	Description
member_ids	No	Array of strings	Backend server IDs.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-1005 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1006 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1007** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1008** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1009** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Enabling backend servers of a VPC channel

```
{
  "member_ids" : [ "b20a5be94ded40cc8f2872ea3005cfb7", "5f918d104dc84480a75166ba99efff21" ]
}
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3023",
  "error_msg" : "The VPC channel does not exist,id:56a7d7358e1b42459c9d730d65b14e59"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.11 Disabling Backend Servers

Function

This API is used to disable backend servers of a VPC channel.

The statuses of backend servers cannot be modified for a reference load balance channel.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/batch-disable

Table 4-1010 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
vpc_channel_id	Yes	String	VPC channel ID.

Request Parameters

Table 4-1011 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1012 Request body parameters

Parameter	Mandatory	Type	Description
member_ids	No	Array of strings	Backend server IDs.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-1013 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1014 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1015 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1016 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1017** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Disabling backend servers of a VPC channel

```
{
  "member_ids" : [ "b20a5be94ded40cc8f2872ea3005cfb7", "5f918d104dc84480a75166ba99efff21" ]
}
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3023",
  "error_msg" : "The VPC channel does not exist,id:56a7d7358e1b42459c9d730d65b14e59"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.12 Modifying VPC Channel Health Check

Function

This API is used to modify the health check configuration of a VPC channel.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/health-config

Table 4-1018 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
vpc_channel_id	Yes	String	VPC channel ID.

Request Parameters

Table 4-1019 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1020 Request body parameters

Parameter	Mandatory	Type	Description
protocol	Yes	String	Protocol for performing health checks on backend servers in the VPC channel. • TCP • HTTP • HTTPS
path	No	String	Destination path for health checks. This parameter is required if protocol is set to http or https.
method	No	String	Request method for health checks. Default: GET

Parameter	Mandatory	Type	Description
port	No	Integer	Destination port for health checks. If this parameter is not specified or set to 0, the host port of the VPC channel is used. If this parameter is set to a non-zero value, the corresponding port is used for health checks. Minimum: 0 Maximum: 65535
threshold_normal	Yes	Integer	Healthy threshold. It refers to the number of consecutive successful checks required for a backend server to be considered healthy. Minimum: 1 Maximum: 10
threshold_abnormal	Yes	Integer	Unhealthy threshold, which refers to the number of consecutive failed checks required for a backend server to be considered unhealthy. Minimum: 1 Maximum: 10
time_interval	Yes	Integer	Interval between consecutive checks. Unit: s. The value must be greater than the value of timeout. Minimum: 1 Maximum: 300

Parameter	Mandatory	Type	Description
http_code	No	String	Response codes for determining a successful HTTP response. The value can be any integer within 100–599 in one of the following formats: • Multiple values, for example, 200,201,202 • Range, for example, 200-299 • Multiple values and ranges, for example, 201,202,210-299. This parameter is required if protocol is set to http.
enable_client_ssl	No	Boolean	Indicates whether to enable two-way authentication. If this function is enabled, the certificate specified in the backend_client_certificate configuration item of the instance is used. Default: false
status	No	Integer	Health check result. • 1: available • 2: unavailable
timeout	Yes	Integer	Timeout for determining whether a health check fails. Unit: s. The value must be less than the value of time_interval. Minimum: 1 Maximum: 30

Response Parameters

Status code: 200

Table 4-1021 Response body parameters

Parameter	Type	Description
protocol	String	Protocol for performing health checks on backend servers in the VPC channel. • TCP • HTTP • HTTPS
path	String	Destination path for health checks. This parameter is required if protocol is set to http or https.
method	String	Request method for health checks. Default: GET
port	Integer	Destination port for health checks. If this parameter is not specified or set to 0, the host port of the VPC channel is used. If this parameter is set to a non-zero value, the corresponding port is used for health checks. Minimum: 0 Maximum: 65535
threshold_normal	Integer	Healthy threshold. It refers to the number of consecutive successful checks required for a backend server to be considered healthy. Minimum: 1 Maximum: 10
threshold_abnormal	Integer	Unhealthy threshold, which refers to the number of consecutive failed checks required for a backend server to be considered unhealthy. Minimum: 1 Maximum: 10
time_interval	Integer	Interval between consecutive checks. Unit: s. The value must be greater than the value of timeout. Minimum: 1 Maximum: 300

Parameter	Type	Description
http_code	String	Response codes for determining a successful HTTP response. The value can be any integer within 100–599 in one of the following formats: • Multiple values, for example, 200,201,202 • Range, for example, 200-299 • Multiple values and ranges, for example, 201,202,210-299. This parameter is required if protocol is set to http.
enable_client_ssl	Boolean	Indicates whether to enable two-way authentication. If this function is enabled, the certificate specified in the backend_client_certificate configuration item of the instance is used. Default: false
status	Integer	Health check result. • 1: available • 2: unavailable
timeout	Integer	Timeout for determining whether a health check fails. Unit: s. The value must be less than the value of time_interval. Minimum: 1 Maximum: 30
vpc_channel_id	String	VPC channel ID.
id	String	Health check ID.
create_time	String	Creation time.

Status code: 400**Table 4-1022** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1023** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1024** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1025** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1026** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Modifying health check configurations of a VPC channel

```
{
  "http_code": "200",
  "path": "/vpc/demo",
  "port": 22,
  "protocol": "http",
}
```

```
"threshold_abnormal" : 5,  
"threshold_normal" : 2,  
"time_interval" : 10,  
"timeout" : 5,  
"enable_client_ssl" : false  
}
```

Example Responses

Status code: 200

OK

```
{  
  "protocol" : "http",  
  "path" : "/vpc/demo",  
  "method" : "GET",  
  "port" : 22,  
  "threshold_abnormal" : 5,  
  "threshold_normal" : 2,  
  "time_interval" : 10,  
  "http_code" : "200",  
  "enable_client_ssl" : false,  
  "status" : 1,  
  "timeout" : 5,  
  "id" : "3b3d02026c5f402d85e8645ea95b0816",  
  "vpc_channel_id" : "d38c55c926ca44c2bfb37886d93b9a0d",  
  "create_time" : "2020-07-23T07:11:57Z"  
}
```

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2001",  
  "error_msg" : "The request parameters must be specified, parameter name:members"  
}
```

Status code: 401

Unauthorized

```
{  
  "error_code" : "APIG.1002",  
  "error_msg" : "Incorrect token or token resolution failed"  
}
```

Status code: 403

Forbidden

```
{  
  "error_code" : "APIG.1005",  
  "error_msg" : "No permissions to request this method"  
}
```

Status code: 404

Not Found

```
{  
  "error_code" : "APIG.3023",  
  "error_msg" : "The VPC channel does not exist,id:56a7d7358e1b42459c9d730d65b14e59"  
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.13 Adding or Updating a Backend Server Group of a VPC Channel

Function

When creating a backend server group for a VPC channel, you can determine whether to associate backend instances with the group to facilitate backend server node management.

If a backend server group with the specified name already exists, the backend server group information is updated. If the request body contains multiple backend server definitions with the same address, the first definition is used.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups

Table 4-1027 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
vpc_channel_id	Yes	String	VPC channel ID.

Request Parameters

Table 4-1028 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1029 Request body parameters

Parameter	Mandatory	Type	Description
member_groups	No	Array of MemberGroupCreate objects	Backend server groups.

Table 4-1030 MemberGroupCreate

Parameter	Mandatory	Type	Description
member_group_name	Yes	String	Name of the VPC channel's backend server group. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.

Parameter	Mandatory	Type	Description
member_group_remark	No	String	Description of the backend server group. Maximum: 255
member_group_weight	No	Integer	Weight of the backend server group. If the server group contains servers and a weight has been set for it, the weight is automatically used to assign weights to servers in this group. Minimum: 0 Maximum: 100
dict_code	No	String	Dictionary code of the backend server group. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). Currently, this parameter is not supported. Minimum: 3 Maximum: 64
microservice_version	No	String	Version of the backend server group. This parameter is supported only when the VPC channel type is microservice. Maximum: 64
microservice_port	No	Integer	Port of the backend server group. This parameter is supported only when the VPC channel type is microservice. If the port number is 0, all addresses in the backend server group use the original load balancing port to inherit logic. Minimum: 0 Maximum: 65535
microservice_labels	No	Array of MicroserviceLabel objects	Tags of the backend server group. This parameter is supported only when the VPC channel type is microservice.

Parameter	Mandatory	Type	Description
reference_vpc_channel_id	No	String	ID of the reference load balance channel. This parameter is supported only when the VPC channel type is reference (vpc_channel_type=reference). Minimum: 0 Maximum: 64

Table 4-1031 MicroserviceLabel

Parameter	Mandatory	Type	Description
label_name	Yes	String	Tag name. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63
label_value	Yes	String	Tag value. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Response Parameters

Status code: 201

Table 4-1032 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.

Parameter	Type	Description
member_groups	Array of MemberGroupInfo objects	Backend server groups of the VPC channel.

Table 4-1033 MemberGroupInfo

Parameter	Type	Description
member_group_name	String	Name of the VPC channel's backend server group. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
member_group_remark	String	Description of the backend server group. Maximum: 255
member_group_weight	Integer	Weight of the backend server group. If the server group contains servers and a weight has been set for it, the weight is automatically used to assign weights to servers in this group. Minimum: 0 Maximum: 100
dict_code	String	Dictionary code of the backend server group. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). Currently, this parameter is not supported. Minimum: 3 Maximum: 64
microservice_version	String	Version of the backend server group. This parameter is supported only when the VPC channel type is microservice. Maximum: 64

Parameter	Type	Description
microservice_port	Integer	Port of the backend server group. This parameter is supported only when the VPC channel type is microservice. If the port number is 0, all addresses in the backend server group use the original load balancing port to inherit logic. Minimum: 0 Maximum: 65535
microservice_labels	Array of MicroserviceLabel objects	Tags of the backend server group. This parameter is supported only when the VPC channel type is microservice.
reference_vpc_channel_id	String	ID of the reference load balance channel. This parameter is supported only when the VPC channel type is reference (vpc_channel_type=reference). Minimum: 0 Maximum: 64
member_group_id	String	ID of the backend server group of the VPC channel.
create_time	String	Time when the backend server group is created.
update_time	String	Time when the backend server group is updated.

Table 4-1034 MicroserviceLabel

Parameter	Type	Description
label_name	String	Tag name. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Parameter	Type	Description
label_value	String	Tag value. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Status code: 400**Table 4-1035** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1036** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1037** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1038 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1039** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

- Creating a backend server group for a VPC channel of the server type

```
{
  "member_groups" : [ {
    "member_group_name" : "vpc_member_group",
    "member_group_weight" : 10
  } ]
}
```

- Creating a backend server group for a VPC channel of the microservice type

```
{
  "member_groups" : [ {
    "member_group_name" : "vpc_member_group",
    "member_group_weight" : 10,
    "microservice_version" : "v1",
    "microservice_port" : 80,
    "microservice_labels" : [ {
      "label_name" : "cluster_id",
      "label_value" : "c429700c-5dc4-482a-9c0e-99f6c0635113"
    } ]
  } ]
}
```

Example Responses

Status code: 201

Created

- Example 1

```
{
  "total" : 1,
  "size" : 1,
  "member_groups" : [ {
    "member_group_name" : "vpc_member_group",
    "member_group_id" : "105c6902457144a4820dff8b1ad63331",
    "member_group_remark" : "",
    "member_group_weight" : 10,
    "create_time" : "2020-07-23T07:24:33Z",

```

```
"update_time" : "2020-07-23T07:24:33Z",
"microservice_version" : "",
"microservice_port" : 0,
"microservice_labels" : [ ]
}]
}
```

- Example 2

```
{
  "total" : 1,
  "size" : 1,
  "member_groups" : [ {
    "member_group_name" : "vpc_member_group",
    "member_group_id" : "105c6902457144a4820dff8b1ad63331",
    "member_group_remark" : "",
    "member_group_weight" : 10,
    "create_time" : "2020-07-23T07:24:33Z",
    "update_time" : "2020-07-23T07:24:33Z",
    "microservice_version" : "v1",
    "microservice_port" : 80,
    "microservice_labels" : [ {
      "label_name" : "cluster_id",
      "label_value" : "c429700c-5dc4-482a-9c0e-99f6c0635113"
    } ]
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2001",
  "error_msg" : "The request parameters must be specified, parameter name:name"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3023",
  "error_msg" : "The VPC channel does not exist,id:56a7d7358e1b42459c9d730d65b14e59"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
}
```

```
"error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.14 Querying Backend Server Groups of a VPC Channel

Function

This API is used to query backend server groups of a VPC channel.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups

Table 4-1040 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Parameter	Mandatory	Type	Description
vpc_channel_id	Yes	String	VPC channel ID.

Table 4-1041 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
dict_code	No	String	Dictionary code. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). This parameter is currently not supported. Minimum: 3 Maximum: 64
member_group_name	No	String	Backend server group name of the VPC channel.
precise_search	No	String	Parameter name for exact matching. Separate multiple parameter names with commas (,). Currently, member_group_name is supported.

Request Parameters

Table 4-1042 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-1043** Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
member_groups	Array of MemberGroupInfo objects	Backend server groups of the VPC channel.

Table 4-1044 MemberGroupInfo

Parameter	Type	Description
member_group_name	String	Name of the VPC channel's backend server group. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
member_groupRemark	String	Description of the backend server group. Maximum: 255

Parameter	Type	Description
member_group_weight	Integer	Weight of the backend server group. If the server group contains servers and a weight has been set for it, the weight is automatically used to assign weights to servers in this group. Minimum: 0 Maximum: 100
dict_code	String	Dictionary code of the backend server group. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). Currently, this parameter is not supported. Minimum: 3 Maximum: 64
microservice_version	String	Version of the backend server group. This parameter is supported only when the VPC channel type is microservice. Maximum: 64
microservice_port	Integer	Port of the backend server group. This parameter is supported only when the VPC channel type is microservice. If the port number is 0, all addresses in the backend server group use the original load balancing port to inherit logic. Minimum: 0 Maximum: 65535
microservice_labels	Array of MicroserviceLabel objects	Tags of the backend server group. This parameter is supported only when the VPC channel type is microservice.
reference_vpc_channel_id	String	ID of the reference load balance channel. This parameter is supported only when the VPC channel type is reference (vpc_channel_type=reference). Minimum: 0 Maximum: 64
member_group_id	String	ID of the backend server group of the VPC channel.
create_time	String	Time when the backend server group is created.

Parameter	Type	Description
update_time	String	Time when the backend server group is updated.

Table 4-1045 MicroserviceLabel

Parameter	Type	Description
label_name	String	Tag name. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63
label_value	String	Tag value. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Status code: 400**Table 4-1046** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1047** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1048** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1049** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1050** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "total" : 1,
  "size" : 1,
  "member_groups" : [ {
    "member_group_name" : "vpc_member_group",
    "member_group_remark" : "remark",
    "member_group_weight" : 1,
    "dict_code" : "",
    "member_group_id" : "105c6902457144a4820dff8b1ad63331",
    "create_time" : "2020-07-23T07:24:33Z",
    "update_time" : "2020-07-23T07:24:33Z",
    "microservice_version" : "",
    "microservice_port" : 0,
```

```
"microservice_labels" : [ ]  
} ]  
}
```

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2001",  
  "error_msg" : "The request parameters must be specified, parameter name:members"  
}
```

Status code: 401

Unauthorized

```
{  
  "error_code" : "APIG.1002",  
  "error_msg" : "Incorrect token or token resolution failed"  
}
```

Status code: 403

Forbidden

```
{  
  "error_code" : "APIG.1005",  
  "error_msg" : "No permissions to request this method"  
}
```

Status code: 404

Not Found

```
{  
  "error_code" : "APIG.3030",  
  "error_msg" : "The instance does not exist,id:56a7d7358e1b42459c9d730d65b14e59"  
}
```

Status code: 500

Internal Server Error

```
{  
  "error_code" : "APIG.9999",  
  "error_msg" : "System error"  
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.15 Querying a Backend Server Group of a VPC Channel

Function

This API is used to query a backend server group of a specified VPC channel.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}

Table 4-1051 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
vpc_channel_id	Yes	String	VPC channel ID.
member_group_id	Yes	String	Backend server group ID of the VPC channel.

Request Parameters

Table 4-1052 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1053 Response body parameters

Parameter	Type	Description
member_group_name	String	Name of the VPC channel's backend server group. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
member_groupRemark	String	Description of the backend server group. Maximum: 255
member_group_weight	Integer	Weight of the backend server group. If the server group contains servers and a weight has been set for it, the weight is automatically used to assign weights to servers in this group. Minimum: 0 Maximum: 100
dict_code	String	Dictionary code of the backend server group. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). Currently, this parameter is not supported. Minimum: 3 Maximum: 64
microservice_version	String	Version of the backend server group. This parameter is supported only when the VPC channel type is microservice. Maximum: 64
microservice_port	Integer	Port of the backend server group. This parameter is supported only when the VPC channel type is microservice. If the port number is 0, all addresses in the backend server group use the original load balancing port to inherit logic. Minimum: 0 Maximum: 65535

Parameter	Type	Description
microservice_labels	Array of MicroserviceLabel objects	Tags of the backend server group. This parameter is supported only when the VPC channel type is microservice.
reference_vpc_channel_id	String	ID of the reference load balance channel. This parameter is supported only when the VPC channel type is reference (vpc_channel_type=reference). Minimum: 0 Maximum: 64
member_group_id	String	ID of the backend server group of the VPC channel.
create_time	String	Time when the backend server group is created.
update_time	String	Time when the backend server group is updated.

Table 4-1054 MicroserviceLabel

Parameter	Type	Description
label_name	String	Tag name. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63
label_value	String	Tag value. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Status code: 400

Table 4-1055 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1056** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1057** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1058** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1059** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "member_group_name" : "vpc_member_group",
  "member_group_id" : "105c6902457144a4820dff8b1ad63331",
  "dict_code" : "",
  "member_group_remark" : "",
  "create_time" : "2020-07-23T07:24:33Z",
  "update_time" : "2020-07-23T07:24:33Z",
  "microservice_version" : "",
  "microservice_port" : 0,
  "microservice_labels" : [ ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2001",
  "error_msg" : "The request parameters must be specified, parameter name:members"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3023",
  "error_msg" : "The VPC channel does not exist,id:56a7d7358e1b42459c9d730d65b14e59"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.16 Deleting a Backend Server Group of a VPC Channel

Function

This API is used to delete a backend server group of a specified VPC channel.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}

Table 4-1060 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
vpc_channel_id	Yes	String	VPC channel ID.

Parameter	Mandatory	Type	Description
member_group_id	Yes	String	Backend server group ID of the VPC channel.

Request Parameters

Table 4-1061 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-1062 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1063 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1064 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1065** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1066** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2001",
  "error_msg" : "The request parameters must be specified, parameter name:members"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404**Not Found**

```
{
  "error_code" : "APIG.3023",
  "error_msg" : "The VPC channel does not exist,id:56a7d7358e1b42459c9d730d65b14e59"
}
```

Status code: 500**Internal Server Error**

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.17.17 Updating a Backend Server Group of a VPC Channel

Function

This API is used to update a backend server group of a VPC channel. If the load balance channel is the Nacos microservice, the server group weight cannot be modified.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}

Table 4-1067 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
vpc_channel_id	Yes	String	VPC channel ID.
member_group_id	Yes	String	Backend server group ID of the VPC channel.

Request Parameters

Table 4-1068 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1069 Request body parameters

Parameter	Mandatory	Type	Description
member_group_name	Yes	String	Name of the VPC channel's backend server group. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.

Parameter	Mandatory	Type	Description
member_group_remark	No	String	Description of the backend server group. Maximum: 255
member_group_weight	No	Integer	Weight of the backend server group. If the server group contains servers and a weight has been set for it, the weight is automatically used to assign weights to servers in this group. Minimum: 0 Maximum: 100
dict_code	No	String	Dictionary code of the backend server group. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). Currently, this parameter is not supported. Minimum: 3 Maximum: 64
microservice_version	No	String	Version of the backend server group. This parameter is supported only when the VPC channel type is microservice. Maximum: 64
microservice_port	No	Integer	Port of the backend server group. This parameter is supported only when the VPC channel type is microservice. If the port number is 0, all addresses in the backend server group use the original load balancing port to inherit logic. Minimum: 0 Maximum: 65535
microservice_labels	No	Array of MicroserviceLabel objects	Tags of the backend server group. This parameter is supported only when the VPC channel type is microservice.

Parameter	Mandatory	Type	Description
reference_vpc_channel_id	No	String	ID of the reference load balance channel. This parameter is supported only when the VPC channel type is reference (vpc_channel_type=reference). Minimum: 0 Maximum: 64

Table 4-1070 MicroserviceLabel

Parameter	Mandatory	Type	Description
label_name	Yes	String	Tag name. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63
label_value	Yes	String	Tag value. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Response Parameters

Status code: 200

Table 4-1071 Response body parameters

Parameter	Type	Description
member_group_name	String	Name of the VPC channel's backend server group. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.

Parameter	Type	Description
member_group_remark	String	Description of the backend server group. Maximum: 255
member_group_weight	Integer	Weight of the backend server group. If the server group contains servers and a weight has been set for it, the weight is automatically used to assign weights to servers in this group. Minimum: 0 Maximum: 100
dict_code	String	Dictionary code of the backend server group. The value can contain letters, digits, hyphens (-), underscores (_), and periods (.). Currently, this parameter is not supported. Minimum: 3 Maximum: 64
microservice_version	String	Version of the backend server group. This parameter is supported only when the VPC channel type is microservice. Maximum: 64
microservice_port	Integer	Port of the backend server group. This parameter is supported only when the VPC channel type is microservice. If the port number is 0, all addresses in the backend server group use the original load balancing port to inherit logic. Minimum: 0 Maximum: 65535
microservice_labels	Array of MicroserviceLabel objects	Tags of the backend server group. This parameter is supported only when the VPC channel type is microservice.
reference_vpc_channel_id	String	ID of the reference load balance channel. This parameter is supported only when the VPC channel type is reference (vpc_channel_type=reference). Minimum: 0 Maximum: 64

Parameter	Type	Description
member_group_id	String	ID of the backend server group of the VPC channel.
create_time	String	Time when the backend server group is created.
update_time	String	Time when the backend server group is updated.

Table 4-1072 MicroserviceLabel

Parameter	Type	Description
label_name	String	Tag name. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63
label_value	String	Tag value. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Status code: 400**Table 4-1073** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1074 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1075** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1076** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1077** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

- Updating a backend server group for a VPC channel of the server type

```
{
  "member_group_name": "vpc_member_group",
  "member_group_weight": 10
}
```

- Updating a backend server group for a VPC channel of the microservice type

```
{
  "member_group_name": "vpc_member_group",
  "member_group_weight": 10,
}
```

```
"microservice_version" : "v1",  
"microservice_port" : 80,  
"microservice_labels" : [ {  
  "label_name" : "cluster_id",  
  "label_value" : "c429700c-5dc4-482a-9c0e-99f6c0635113"  
} ]  
}
```

Example Responses

Status code: 200

OK

- Example 1

```
{  
  "member_group_name" : "vpc_member_group",  
  "member_group_id" : "105c6902457144a4820dff8b1ad63331",  
  "member_group_remark" : "",  
  "member_group_weight" : 10,  
  "create_time" : "2020-07-23T07:24:33Z",  
  "update_time" : "2020-07-23T07:24:33Z",  
  "microservice_version" : "",  
  "microservice_port" : 0,  
  "microservice_labels" : [ ]  
}
```

- Example 2

```
{  
  "member_group_name" : "vpc_member_group",  
  "member_group_id" : "105c6902457144a4820dff8b1ad63331",  
  "member_group_remark" : "",  
  "member_group_weight" : 10,  
  "create_time" : "2020-07-23T07:24:33Z",  
  "update_time" : "2020-07-23T07:24:33Z",  
  "microservice_version" : "v1",  
  "microservice_port" : 80,  
  "microservice_labels" : [ {  
    "label_name" : "cluster_id",  
    "label_value" : "c429700c-5dc4-482a-9c0e-99f6c0635113"  
  } ]  
}
```

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2001",  
  "error_msg" : "The request parameters must be specified, parameter name:members"  
}
```

Status code: 401

Unauthorized

```
{  
  "error_code" : "APIG.1002",  
  "error_msg" : "Incorrect token or token resolution failed"  
}
```

Status code: 403

Forbidden

```
{  
  "error_code" : "APIG.1005",  
}
```

```
"error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3023",
  "error_msg" : "The VPC channel does not exist,id:56a7d7358e1b42459c9d730d65b14e59"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.18 Monitoring Information Query

4.18.1 Querying API Calls Within a Period

Function

This API is used to query the number of times APIs in an API group are called within a period. The query is based on 1 minute. If the time range is within one hour, the server returns the number of API calls made every minute.

** NOTE**

For security purposes, clear your operation records, including but not limited to records in the `~/.bash_history` and `/var/log/messages` directories (if any), after running the curl command on the server to query information.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/statistics/api/latest

Table 4-1078 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1079 Query Parameters

Parameter	Mandatory	Type	Description
api_id	Yes	String	API ID.
duration	Yes	String	Time range (unit: h or m). For example, 1h refers to the latest 1 hour and 1m refers to the latest 1 minute.

Request Parameters

Table 4-1080 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1081 Response body parameters

Parameter	Type	Description
code	String	Response code.
msg	String	Response message.
start_time	Long	Timestamp (UTC) of the start time.
end_time	Long	Timestamp (UTC) of the end time.
list	Array of StatisticsAPI objects	Statistic data.

Table 4-1082 StatisticsAPI

Parameter	Type	Description
max_latency	Integer	Maximum latency. Unit: ms
avg_latency	Float	Average latency. Unit: ms
req_count	Integer	Total number of requests.
req_count2xx	Integer	Total number of 2xx response codes.
req_count4xx	Integer	Total number of 4xx response codes.
req_count5xx	Integer	Total number of 5xx response codes.
req_count_error	Integer	Errors.
max_inner_latency	Integer	Maximum gateway latency. Unit: ms
avg_inner_latency	Float	Average gateway latency. Unit: ms
max_backend_latency	Integer	Maximum backend latency.
avg_backend_latency	Float	Average backend latency.
output_throughput	Long	Downstream throughput (bytes).
input_throughput	Long	Upstream throughput (bytes).
current_minute	Long	Timestamp (UTC) of API access.
cycle	String	Statistical period.

Parameter	Type	Description
api_id	String	API ID.
group_id	String	API group ID.
provider	String	API provider.
req_time	String	Request time.
register_time	String	Recording time.
status	Integer	Status.

Status code: 400**Table 4-1083** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1084** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1085** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1086 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1087** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "code" : "APIG.0000",
  "start_time" : 1595573280,
  "end_time" : 1595576820,
  "list" : [ {
    "api_id" : "39bce6d25a3f470e8cf7b2c97174f7d9",
    "avg_backend_latency" : 2.71,
    "avg_inner_latency" : 1.57,
    "avg_latency" : 4.14,
    "current_minute" : 1595576640,
    "cycle" : "MINUTE",
    "group_id" : "d0fc4e40b7d1492cba802f667c7c7226",
    "input_throughput" : 1071,
    "max_backend_latency" : 6,
    "max_inner_latency" : 8,
    "max_latency" : 14,
    "output_throughput" : 3790,
    "provider" : "73d69ae0cfcf460190522d06b60f05ad",
    "register_time" : "2020-07-24 15:44:56",
    "req_count" : 7,
    "req_count2xx" : 0,
    "req_count4xx" : 6,
    "req_count5xx" : 1,
    "req_count_error" : 7,
    "req_time" : "2020-07-24 15:44:00",
    "status" : 1
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:api_id. Please refer to the support documentation"
}
```

Status code: 401**Unauthorized**

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403**Forbidden**

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404**Not Found**

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "API 39bce6d25a3f470e8cf7b2c97174f7d9 does not exist"
}
```

Status code: 500**Internal Server Error**

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.18.2 Querying Monitoring Data

Function

This API is used to query the monitoring metric data at a specified granularity in a specified period of time.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/metric-data

Table 4-1088 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1089 Query Parameters

Parameter	Mandatory	Type	Description
dim	Yes	String	Metric dimension. - inbound_eip: Inbound public network bandwidth, which is supported only by gateways that support load balancing. - outbound_eip: Outbound public network bandwidth.

Parameter	Mandatory	Type	Description
metric_name	Yes	String	Metric name. • upstream_bandwidth: Outbound bandwidth. • downstream_bandwidth: Inbound bandwidth. • upstream_bandwidth_usage : Outbound bandwidth usage. • downstream_bandwidth_usage: Inbound bandwidth usage. • up_stream: Outbound traffic. • down_stream: Inbound traffic.
from	Yes	String	Start time of the query. The time is a UNIX timestamp and the unit is ms.
to	Yes	String	End time of the query. The time is a UNIX timestamp and the unit is ms. The value of parameter from must be earlier than that of parameter to.
period	Yes	Integer	Monitoring data granularity. • 1: Real-time data. • 300: 5 minutes. • 1200: 20 minutes. • 3600: 1 hour. • 14400: 4 hours. • 86400: 1 day.

Parameter	Mandatory	Type	Description
filter	Yes	String	Data rollup mode. • average: Average value of the metric data in the rollup period. • max: Maximum value of the metric data in the rollup period. • min: Minimum value of the metric data in the rollup period. • sum: Sum of the metric data in the rollup period. • variance: Variance value of the metric data in the rollup period.

Request Parameters

Table 4-1090 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1091 Response body parameters

Parameter	Type	Description
datapoints	Array of MetricData objects	Metric data.

Table 4-1092 MetricData

Parameter	Type	Description
average	Integer	Average value of metric data within a rollup period. This parameter is supported only when the value of filter in the request is average.
max	Integer	Maximum value of metric data within a rollup period. This parameter is supported only when the value of filter in the request is max.
min	Integer	Minimum value of metric data within a rollup period. This parameter is supported only when the value of filter in the request is min.
sum	Integer	Sum of metric data within a rollup period. This parameter is supported only when the value of filter in the request is sum.
variance	Integer	Variance value of metric data within a rollup period. This parameter is supported only when the value of filter in the request is variance.
timestamp	Long	Time when the metric is collected. It is a UNIX timestamp in milliseconds.
unit	String	Metric unit.

Status code: 400**Table 4-1093** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1094** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 403**Table 4-1095** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1096** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1097** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "datapoints" : [ {
    "average" : 5,
    "timestamp" : 1665304920000,
```

```
"unit" : "Byte"
} ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:api_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "API 39bce6d25a3f470e8cf7b2c97174f7d9 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.18.3 Querying API Calls Under an API Group in the Last One Hour

Function

This API is used to query the total number of times all APIs in an API group are called based on the API group ID. The query is based on 1 minute. If the time range is within one hour, the server returns the number of API calls made every minute.

NOTE

For security purposes, clear your operation records, including but not limited to records in the `~/.bash_history` and `/var/log/messages` directories (if any), after running the curl command on the server to query information.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/statistics/group/latest

Table 4-1098 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1099 Query Parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	API group ID.

Request Parameters

Table 4-1100 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-1101** Response body parameters

Parameter	Type	Description
code	String	Response code.
msg	String	Response message.
start_time	Long	Timestamp (UTC) of the start time.
end_time	Long	Timestamp (UTC) of the end time.
list	Array of StatisticsGroup objects	Statistic data.

Table 4-1102 StatisticsGroup

Parameter	Type	Description
max_latency	Integer	Maximum latency. Unit: ms
avg_latency	Float	Average latency. Unit: ms
req_count	Integer	Total number of requests.
req_count2xx	Integer	Total number of 2xx response codes.
req_count4xx	Integer	Total number of 4xx response codes.
req_count5xx	Integer	Total number of 5xx response codes.
req_count_error	Integer	Errors.

Parameter	Type	Description
output_throughput	Long	Downstream throughput (bytes).
input_throughput	Long	Upstream throughput (bytes).
current_minute	Long	Timestamp (UTC) of API access.
group_id	String	API group ID.
provider	String	API provider.
req_time	String	Request time.
register_time	String	Recording time.

Status code: 400**Table 4-1103** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1104** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1105** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1106 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1107 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "code" : "APIG.0000",
  "start_time" : 1595574540,
  "end_time" : 1595578080,
  "list" : [ {
    "avg_latency" : 4.14,
    "current_minute" : 1595576640,
    "group_id" : "d0fc4e40b7d1492cba802f667c7c7226",
    "input_throughput" : 1071,
    "max_latency" : 14,
    "output_throughput" : 3790,
    "provider" : "73d69ae0cfcf460190522d06b60f05ad",
    "register_time" : "2020-07-24 15:44:56",
    "req_count" : 7,
    "req_count2xx" : 0,
    "req_count4xx" : 6,
    "req_count5xx" : 1,
    "req_count_error" : 7,
    "req_time" : "2020-07-24 15:44:00"
  }, {
    "avg_latency" : 3.67,
    "current_minute" : 1595577900,
    "group_id" : "d0fc4e40b7d1492cba802f667c7c7226",
    "input_throughput" : 915,
    "max_latency" : 6,
    "output_throughput" : 2763,
    "provider" : "73d69ae0cfcf460190522d06b60f05ad",
    "register_time" : "2020-07-24 16:05:12",
    "req_count" : 6,
    "req_count2xx" : 3,
    "req_count4xx" : 0,
```

```
{  "req_count5xx" : 3,  "req_count_error" : 3,  "req_time" : "2020-07-24 16:05:00"  } ]}
```

Status code: 400

Bad Request

```
{  "error_code" : "APIG.2012",  "error_msg" : "Invalid parameter value,parameterName:group_id. Please refer to the support documentation"}
```

Status code: 401

Unauthorized

```
{  "error_code" : "APIG.1002",  "error_msg" : "Incorrect token or token resolution failed"}
```

Status code: 403

Forbidden

```
{  "error_code" : "APIG.1005",  "error_msg" : "No permissions to request this method"}
```

Status code: 404

Not Found

```
{  "error_code" : "APIG.3001",  "error_msg" : "API group d0fc4e40b7d1492cba802f667c7c7226 does not exist"}
```

Status code: 500

Internal Server Error

```
{  "error_code" : "APIG.9999",  "error_msg" : "System error"}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

Status Code	Description
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.19 Group Response Management

4.19.1 Creating a Group Response

Function

This API is used to create a response for an API group.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses

Table 4-1108 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.

Request Parameters

Table 4-1109 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1110 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Response name. Enter 1 to 64 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.

Parameter	Mandatory	Type	Description
responses	No	Map<String, ResponseInfo >	Response type definition. key indicates the error type. Options of key: • AUTH_FAILURE: Authentication failed. • AUTH_HEADER_MISSING: The identity source is missing. • AUTHORIZER_FAILURE: Custom authentication failed. • AUTHORIZER_CONF_FAILURE: Custom authorizer error. • AUTHORIZER_IDENTITY_FAILURE: The identity source of the custom authorizer is invalid. • BACKEND_UNAVAILABLE: The backend is unavailable. • BACKEND_TIMEOUT: Backend timed out. • THROTTLED: The request was rejected due to request throttling. • UNAUTHORIZED: The app you are using has not been authorized to call the API. • ACCESS_DENIED: Access denied. • NOT_FOUND: No API is found. • REQUEST_PARAMETERS_FAILURE: Invalid request parameter. • DEFAULT_4XX: Default 4XX error occurred. • DEFAULT_5XX: Default 5XX error occurred. • THIRD_AUTH_FAILURE: Third-party authentication failed. • THIRD_AUTH_IDENTITY_FAILURE: Identity source of the third-party authorizer is invalid.

Parameter	Mandatory	Type	Description
			• THIRD_AUTH_CONF_FAILURE: Third-party authorizer configuration error. • ORCHESTRATION_PARAMETER_NOT_FOUND: No parameters are input to match the parameter orchestration rule, causing orchestration failure. • ORCHESTRATION_FAILURE: Input parameters cannot match orchestration rules, causing orchestration failure. Each error type is in JSON format.

Table 4-1111 ResponseInfo

Parameter	Mandatory	Type	Description
status	No	Integer	HTTP status code of the response. The value ranges from 200 to 599, but cannot be 444.
body	No	String	Response body template.
headers	No	Array of ResponseInfo Header objects	Custom response header. Array Length: 0 - 10

Table 4-1112 ResponseInfoHeader

Parameter	Mandatory	Type	Description
key	No	String	Key of the custom group response header, which can contain 1 to 128 characters of letters, digits, and hyphens (-).
value	No	String	Value of the custom group response header, which is a string of 1 to 1,024 characters. Minimum: 1 Maximum: 1024

Response Parameters

Status code: 201

Table 4-1113 Response body parameters

Parameter	Type	Description
name	String	Response name.

Parameter	Type	Description
responses	Map<String, ResponseInfoResp >	Response type definition. key indicates the error type. Options of key: • AUTH_FAILURE: Authentication failed. • AUTH_HEADER_MISSING: The identity source is missing. • AUTHORIZER_FAILURE: Custom authentication failed. • AUTHORIZER_CONF_FAILURE: Custom authorizer error. • AUTHORIZER_IDENTITY_FAILURE: The identity source of the custom authorizer is invalid. • BACKEND_UNAVAILABLE: The backend is unavailable. • BACKEND_TIMEOUT: Backend timed out. • THROTTLED: The request was rejected due to request throttling. • UNAUTHORIZED: The app you are using has not been authorized to call the API. • ACCESS_DENIED: Access denied. • NOT_FOUND: No API is found. • REQUEST_PARAMETERS_FAILURE: Invalid request parameter. • DEFAULT_4XX: Default 4XX error occurred. • DEFAULT_5XX: Default 5XX error occurred. • THIRD_AUTH_FAILURE: Third-party authentication failed. • THIRD_AUTH_IDENTITY_FAILURE: Identity source of the third-party authorizer is invalid. • THIRD_AUTH_CONF_FAILURE: Third-party authorizer configuration error. • ORCHESTRATION_PARAMETER_NOT_FOUND: No parameters are input to match the parameter orchestration rule, causing orchestration failure. • ORCHESTRATION_FAILURE: Input parameters cannot match

Parameter	Type	Description
		orchestration rules, causing orchestration failure. Each error type is in JSON format.
id	String	Response ID.
default	Boolean	Indicates whether the group response is the default response.
create_time	String	Creation time.
update_time	String	Update time.

Table 4-1114 ResponseInfoResp

Parameter	Type	Description
status	Integer	HTTP status code of the response. The value ranges from 200 to 599, but cannot be 444.
body	String	Response body template.
headers	Array of ResponseInfoHeader objects	Custom response header. Array Length: 0 - 10
default	Boolean	Indicates whether the response is the default response.

Table 4-1115 ResponseInfoHeader

Parameter	Type	Description
key	String	Key of the custom group response header, which can contain 1 to 128 characters of letters, digits, and hyphens (-).
value	String	Value of the custom group response header, which is a string of 1 to 1,024 characters. Minimum: 1 Maximum: 1024

Status code: 400

Table 4-1116 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1117** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1118** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1119** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1120** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Creating a response for an API group

```
{
  "name" : "response_demo"
}
```

Example Responses

Status code: 201

Created

```
{
  "create_time" : "2020-08-12T14:52:02.829753306+08:00",
  "update_time" : "2020-08-12T14:52:02.829753306+08:00",
  "default" : false,
  "id" : "e839b367e10f4ab19d1c5008e476b83a",
  "name" : "response_demo",
  "responses" : {
    "ACCESS_DENIED" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 403
    },
    "AUTHORIZER_CONF_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 500
    },
    "AUTHORIZER_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 500
    },
    "AUTHORIZER_IDENTITY_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 401
    },
    "AUTH_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 401
    },
    "AUTH_HEADER_MISSING" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 401
    },
    "BACKEND_TIMEOUT" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 504
    },
    "BACKEND_UNAVAILABLE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 502
    }
  }
}
```

```
    },
    "DEFAULT_4XX" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true
    },
    },
    "DEFAULT_5XX" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true
    },
    },
    "NOT_FOUND" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 404
    },
    },
    "REQUEST_PARAMETERS_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 400
    },
    },
    "THROTTLED" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 429
    },
    },
    "UNAUTHORIZED" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 401
    },
    },
    "THIRD_AUTH_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 401
    },
    },
    "THIRD_AUTH_IDENTITY_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 401
    },
    },
    "THIRD_AUTH_CONF_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 500
    }
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3001",
  "error_msg" : "API group c77f5e81d9cb4424bf704ef2b0ac7600 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.19.2 Querying Group Response Details

Function

This API is used to query the details of a response defined for an API group.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}

Table 4-1121 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.
response_id	Yes	String	Response ID.

Request Parameters

Table 4-1122 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1123 Response body parameters

Parameter	Type	Description
name	String	Response name.

Parameter	Type	Description
responses	Map<String, ResponseInfoResp >	Response type definition. key indicates the error type. Options of key: • AUTH_FAILURE: Authentication failed. • AUTH_HEADER_MISSING: The identity source is missing. • AUTHORIZER_FAILURE: Custom authentication failed. • AUTHORIZER_CONF_FAILURE: Custom authorizer error. • AUTHORIZER_IDENTITY_FAILURE: The identity source of the custom authorizer is invalid. • BACKEND_UNAVAILABLE: The backend is unavailable. • BACKEND_TIMEOUT: Backend timed out. • THROTTLED: The request was rejected due to request throttling. • UNAUTHORIZED: The app you are using has not been authorized to call the API. • ACCESS_DENIED: Access denied. • NOT_FOUND: No API is found. • REQUEST_PARAMETERS_FAILURE: Invalid request parameter. • DEFAULT_4XX: Default 4XX error occurred. • DEFAULT_5XX: Default 5XX error occurred. • THIRD_AUTH_FAILURE: Third-party authentication failed. • THIRD_AUTH_IDENTITY_FAILURE: Identity source of the third-party authorizer is invalid. • THIRD_AUTH_CONF_FAILURE: Third-party authorizer configuration error. • ORCHESTRATION_PARAMETER_NOT_FOUND: No parameters are input to match the parameter orchestration rule, causing orchestration failure. • ORCHESTRATION_FAILURE: Input parameters cannot match

Parameter	Type	Description
		orchestration rules, causing orchestration failure. Each error type is in JSON format.
id	String	Response ID.
default	Boolean	Indicates whether the group response is the default response.
create_time	String	Creation time.
update_time	String	Update time.

Table 4-1124 ResponseInfoResp

Parameter	Type	Description
status	Integer	HTTP status code of the response. The value ranges from 200 to 599, but cannot be 444.
body	String	Response body template.
headers	Array of ResponseInfoHeader objects	Custom response header. Array Length: 0 - 10
default	Boolean	Indicates whether the response is the default response.

Table 4-1125 ResponseInfoHeader

Parameter	Type	Description
key	String	Key of the custom group response header, which can contain 1 to 128 characters of letters, digits, and hyphens (-).
value	String	Value of the custom group response header, which is a string of 1 to 1,024 characters. Minimum: 1 Maximum: 1024

Status code: 400

Table 4-1126 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1127** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1128** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1129** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1130** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

Created

```
{
  "create_time": "2020-08-12T06:52:02Z",
  "update_time": "2020-08-12T06:52:02Z",
  "default": false,
  "id": "e839b367e10f4ab19d1c5008e476b83a",
  "name": "response_demo",
  "responses": {
    "ACCESS_DENIED": {
      "body": "{\"error_code\":\"$context.error.code\",\"error_msg\":\"$context.error.message\",\"request_id\":\"$context.requestId\"}",
      "default": true,
      "status": 403
    },
    "AUTHORIZER_CONF_FAILURE": {
      "body": "{\"error_code\":\"$context.error.code\",\"error_msg\":\"$context.error.message\",\"request_id\":\"$context.requestId\"}",
      "default": true,
      "status": 500
    },
    "AUTHORIZER_FAILURE": {
      "body": "{\"error_code\":\"$context.error.code\",\"error_msg\":\"$context.error.message\",\"request_id\":\"$context.requestId\"}",
      "default": true,
      "status": 500
    },
    "AUTHORIZER_IDENTITY_FAILURE": {
      "body": "{\"error_code\":\"$context.error.code\",\"error_msg\":\"$context.error.message\",\"request_id\":\"$context.requestId\"}",
      "default": true,
      "status": 401
    },
    "AUTH_FAILURE": {
      "body": "{\"error_code\":\"$context.error.code\",\"error_msg\":\"$context.error.message\",\"request_id\":\"$context.requestId\"}",
      "default": true,
      "status": 401
    },
    "AUTH_HEADER_MISSING": {
      "body": "{\"error_code\":\"$context.error.code\",\"error_msg\":\"$context.error.message\",\"request_id\":\"$context.requestId\"}",
      "default": true,
      "status": 401
    },
    "BACKEND_TIMEOUT": {
      "body": "{\"error_code\":\"$context.error.code\",\"error_msg\":\"$context.error.message\",\"request_id\":\"$context.requestId\"}",
      "default": true,
      "status": 504
    },
    "BACKEND_UNAVAILABLE": {
      "body": "{\"error_code\":\"$context.error.code\",\"error_msg\":\"$context.error.message\",\"request_id\":\"$context.requestId\"}",
      "default": true,
      "status": 502
    },
    "DEFAULT_4XX": {
      "body": "{\"error_code\":\"$context.error.code\",\"error_msg\":\"$context.error.message\",\"request_id\":\"$context.requestId\"}",

```

```
"default" : true
},
"DEFAULT_5XX" : {
  "body" : "{\\"error_code\\":\\"$context.error.code\\",\\"error_msg\\":\\"$context.error.message\\",\\"request_id\\":\\"$context.requestId\\"}",
  "default" : true
},
"NOT_FOUND" : {
  "body" : "{\\"error_code\\":\\"$context.error.code\\",\\"error_msg\\":\\"$context.error.message\\",\\"request_id\\":\\"$context.requestId\\"}",
  "default" : true,
  "status" : 404
},
"REQUEST_PARAMETERS_FAILURE" : {
  "body" : "{\\"error_code\\":\\"$context.error.code\\",\\"error_msg\\":\\"$context.error.message\\",\\"request_id\\":\\"$context.requestId\\"}",
  "default" : true,
  "status" : 400
},
"THROTTLED" : {
  "body" : "{\\"error_code\\":\\"$context.error.code\\",\\"error_msg\\":\\"$context.error.message\\",\\"request_id\\":\\"$context.requestId\\"}",
  "default" : true,
  "status" : 429
},
"UNAUTHORIZED" : {
  "body" : "{\\"error_code\\":\\"$context.error.code\\",\\"error_msg\\":\\"$context.error.message\\",\\"request_id\\":\\"$context.requestId\\"}",
  "default" : true,
  "status" : 401
},
"THIRD_AUTH_FAILURE" : {
  "body" : "{\\"error_code\\":\\"$context.error.code\\",\\"error_msg\\":\\"$context.error.message\\",\\"request_id\\":\\"$context.requestId\\"}",
  "default" : true,
  "status" : 401
},
"THIRD_AUTH_IDENTITY_FAILURE" : {
  "body" : "{\\"error_code\\":\\"$context.error.code\\",\\"error_msg\\":\\"$context.error.message\\",\\"request_id\\":\\"$context.requestId\\"}",
  "default" : true,
  "status" : 401
},
"THIRD_AUTH_CONF_FAILURE" : {
  "body" : "{\\"error_code\\":\\"$context.error.code\\",\\"error_msg\\":\\"$context.error.message\\",\\"request_id\\":\\"$context.requestId\\"}",
  "default" : true,
  "status" : 500
}
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:group_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3001",
  "error_msg" : "API group c77f5e81d9cb4424bf704ef2b0ac7600 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.19.3 Modifying a Group Response

Function

This API is used to modify a response of an API group.

Calling MethodFor details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}

Table 4-1131 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.
response_id	Yes	String	Response ID.

Request Parameters

Table 4-1132 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1133 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Response name. Enter 1 to 64 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.

Parameter	Mandatory	Type	Description
responses	No	Map<String, ResponseInfo >	Response type definition. key indicates the error type. Options of key: • AUTH_FAILURE: Authentication failed. • AUTH_HEADER_MISSING: The identity source is missing. • AUTHORIZER_FAILURE: Custom authentication failed. • AUTHORIZER_CONF_FAILURE: Custom authorizer error. • AUTHORIZER_IDENTITY_FAILURE: The identity source of the custom authorizer is invalid. • BACKEND_UNAVAILABLE: The backend is unavailable. • BACKEND_TIMEOUT: Backend timed out. • THROTTLED: The request was rejected due to request throttling. • UNAUTHORIZED: The app you are using has not been authorized to call the API. • ACCESS_DENIED: Access denied. • NOT_FOUND: No API is found. • REQUEST_PARAMETERS_FAILURE: Invalid request parameter. • DEFAULT_4XX: Default 4XX error occurred. • DEFAULT_5XX: Default 5XX error occurred. • THIRD_AUTH_FAILURE: Third-party authentication failed. • THIRD_AUTH_IDENTITY_FAILURE: Identity source of the third-party authorizer is invalid.

Parameter	Mandatory	Type	Description
			• THIRD_AUTH_CONF_FAILURE: Third-party authorizer configuration error. • ORCHESTRATION_PARAMETER_NOT_FOUND: No parameters are input to match the parameter orchestration rule, causing orchestration failure. • ORCHESTRATION_FAILURE: Input parameters cannot match orchestration rules, causing orchestration failure. Each error type is in JSON format.

Table 4-1134 ResponseInfo

Parameter	Mandatory	Type	Description
status	No	Integer	HTTP status code of the response. The value ranges from 200 to 599, but cannot be 444.
body	No	String	Response body template.
headers	No	Array of ResponseInfo Header objects	Custom response header. Array Length: 0 - 10

Table 4-1135 ResponseInfoHeader

Parameter	Mandatory	Type	Description
key	No	String	Key of the custom group response header, which can contain 1 to 128 characters of letters, digits, and hyphens (-).
value	No	String	Value of the custom group response header, which is a string of 1 to 1,024 characters. Minimum: 1 Maximum: 1024

Response Parameters

Status code: 200

Table 4-1136 Response body parameters

Parameter	Type	Description
name	String	Response name.

Parameter	Type	Description
responses	Map<String, ResponseInfoResp >	Response type definition. key indicates the error type. Options of key: • AUTH_FAILURE: Authentication failed. • AUTH_HEADER_MISSING: The identity source is missing. • AUTHORIZER_FAILURE: Custom authentication failed. • AUTHORIZER_CONF_FAILURE: Custom authorizer error. • AUTHORIZER_IDENTITY_FAILURE: The identity source of the custom authorizer is invalid. • BACKEND_UNAVAILABLE: The backend is unavailable. • BACKEND_TIMEOUT: Backend timed out. • THROTTLED: The request was rejected due to request throttling. • UNAUTHORIZED: The app you are using has not been authorized to call the API. • ACCESS_DENIED: Access denied. • NOT_FOUND: No API is found. • REQUEST_PARAMETERS_FAILURE: Invalid request parameter. • DEFAULT_4XX: Default 4XX error occurred. • DEFAULT_5XX: Default 5XX error occurred. • THIRD_AUTH_FAILURE: Third-party authentication failed. • THIRD_AUTH_IDENTITY_FAILURE: Identity source of the third-party authorizer is invalid. • THIRD_AUTH_CONF_FAILURE: Third-party authorizer configuration error. • ORCHESTRATION_PARAMETER_NOT_FOUND: No parameters are input to match the parameter orchestration rule, causing orchestration failure. • ORCHESTRATION_FAILURE: Input parameters cannot match

Parameter	Type	Description
		orchestration rules, causing orchestration failure. Each error type is in JSON format.
id	String	Response ID.
default	Boolean	Indicates whether the group response is the default response.
create_time	String	Creation time.
update_time	String	Update time.

Table 4-1137 ResponseInfoResp

Parameter	Type	Description
status	Integer	HTTP status code of the response. The value ranges from 200 to 599, but cannot be 444.
body	String	Response body template.
headers	Array of ResponseInfoHeader objects	Custom response header. Array Length: 0 - 10
default	Boolean	Indicates whether the response is the default response.

Table 4-1138 ResponseInfoHeader

Parameter	Type	Description
key	String	Key of the custom group response header, which can contain 1 to 128 characters of letters, digits, and hyphens (-).
value	String	Value of the custom group response header, which is a string of 1 to 1,024 characters. Minimum: 1 Maximum: 1024

Status code: 400

Table 4-1139 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1140** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1141** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1142** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1143** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Modifying a response of an API group

```
{
  "name" : "response_demo"
}
```

Example Responses

Status code: 200

OK

```
{
  "create_time" : "2020-08-12T06:52:02Z",
  "update_time" : "2020-08-12T15:22:21.929863859+08:00",
  "default" : false,
  "id" : "e839b367e10f4ab19d1c5008e476b83a",
  "name" : "response_demo",
  "responses" : {
    "ACCESS_DENIED" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 403
    },
    "AUTHORIZER_CONF_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 500
    },
    "AUTHORIZER_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 500
    },
    "AUTHORIZER_IDENTITY_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 401
    },
    "AUTH_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 401
    },
    "AUTH_HEADER_MISSING" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 401
    },
    "BACKEND_TIMEOUT" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 504
    },
    "BACKEND_UNAVAILABLE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 502
    }
  }
}
```

```
    },
    "DEFAULT_4XX" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true
    },
    },
    "DEFAULT_5XX" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true
    },
    },
    "NOT_FOUND" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 404
    },
    },
    "REQUEST_PARAMETERS_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 400
    },
    },
    "THROTTLED" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 429
    },
    },
    "UNAUTHORIZED" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 401
    },
    },
    "THIRD_AUTH_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 401
    },
    },
    "THIRD_AUTH_IDENTITY_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 401
    },
    },
    "THIRD_AUTH_CONF_FAILURE" : {
      "body" : "{ \"error_code\": \"${context.error.code}\", \"error_msg\": \"${context.error.message}\", \"request_id\": \"${context.requestId}\" }",
      "default" : true,
      "status" : 500
    }
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3001",
  "error_msg" : "API group c77f5e81d9cb4424bf704ef2b0ac7600 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.19.4 Deleting a Group Response

Function

This API is used to delete a group response of an API group.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}

Table 4-1144 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.
response_id	Yes	String	Response ID.

Request Parameters

Table 4-1145 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-1146 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 401**Table 4-1147** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1148** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1149** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1150** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:group_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3001",
  "error_msg" : "API group c77f5e81d9cb4424bf704ef2b0ac7600 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.19.5 Querying the Response of an Error Type

Function

This API is used to query the response of an error type defined for an API group.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}/{response_type}

Table 4-1151 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.
response_id	Yes	String	Response ID.

Parameter	Mandatory	Type	Description
response_type	Yes	String	Error type. Options: • AUTH_FAILURE: IAM or app authentication failed. • AUTH_HEADER_MISSING: The identity source is missing. • AUTHORIZER_FAILURE: Custom authentication failed. • AUTHORIZER_CONF_FAILURE: A custom authorizer error has occurred. For example, communication failed or an error response was returned. • AUTHORIZER_IDENTITY_FAILURE: The identity source of the frontend custom authorizer is missing or invalid. • BACKEND_UNAVAILABLE: The backend is unavailable due to communication error. • BACKEND_TIMEOUT: Communication with the backend timed out. • THROTTLED: The request was rejected due to throttling. • UNAUTHORIZED: The credential you use is not authorized to call the API. • ACCESS_DENIED: Access denied. For example, the access control policy is triggered or an attack is detected. • NOT_FOUND: No API is matched. • REQUEST_PARAMETERS_FAILURE: Invalid request parameter or unsupported HTTP method. • DEFAULT_4XX: Another 4XX error occurred.

Parameter	Mandatory	Type	Description
			• DEFAULT_5XX: Another 5XX error occurred. • THIRD_AUTH_FAILURE: Third-party authentication failed. • THIRD_AUTH_IDENTITY_FAILURE: The identity source of the third-party authorizer is missing or invalid. • THIRD_AUTH_CONF_FAILURE: A third-party authorizer error has occurred. For example, communication failed or an error response was returned. • ORCHESTRATION_PARAMETER_NOT_FOUND: Parameter orchestration failed. No input parameter is found in the request. • ORCHESTRATION_FAILURE: Parameter orchestration failed. No orchestration rule to match.

Request Parameters

Table 4-1152 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1153 Response body parameters

Parameter	Type	Description
{User defined key}	Map<String, ResponseInfoResp >	

Table 4-1154 ResponseInfoResp

Parameter	Type	Description
status	Integer	HTTP status code of the response. The value ranges from 200 to 599, but cannot be 444.
body	String	Response body template.
headers	Array of ResponseInfoHeader objects	Custom response header. Array Length: 0 - 10
default	Boolean	Indicates whether the response is the default response.

Table 4-1155 ResponseInfoHeader

Parameter	Type	Description
key	String	Key of the custom group response header, which can contain 1 to 128 characters of letters, digits, and hyphens (-).
value	String	Value of the custom group response header, which is a string of 1 to 1,024 characters. Minimum: 1 Maximum: 1024

Status code: 400**Table 4-1156** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1157** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1158** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1159** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1160** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "ACCESS_DENIED" : {
    "body" : "{ \"error_code\" : \"$context.error.code\", \"error_msg\" : \"$context.error.message\", \"request_id\" : \"$context.requestId\" }",
    "default" : true,
    "status" : 403
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:group_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3001",
  "error_msg" : "API group c77f5e81d9cb4424bf704ef2b0ac7600 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request

Status Code	Description
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.19.6 Modifying the Response of an Error Type

Function

This API is used to modify the response of an error type defined for an API group.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}/{response_type}

Table 4-1161 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.
response_id	Yes	String	Response ID.

Parameter	Mandatory	Type	Description
response_type	Yes	String	Error type. Options: • AUTH_FAILURE: IAM or app authentication failed. • AUTH_HEADER_MISSING: The identity source is missing. • AUTHORIZER_FAILURE: Custom authentication failed. • AUTHORIZER_CONF_FAILURE: A custom authorizer error has occurred. For example, communication failed or an error response was returned. • AUTHORIZER_IDENTITY_FAILURE: The identity source of the frontend custom authorizer is missing or invalid. • BACKEND_UNAVAILABLE: The backend is unavailable due to communication error. • BACKEND_TIMEOUT: Communication with the backend timed out. • THROTTLED: The request was rejected due to throttling. • UNAUTHORIZED: The credential you use is not authorized to call the API. • ACCESS_DENIED: Access denied. For example, the access control policy is triggered or an attack is detected. • NOT_FOUND: No API is matched. • REQUEST_PARAMETERS_FAILURE: Invalid request parameter or unsupported HTTP method. • DEFAULT_4XX: Another 4XX error occurred.

Parameter	Mandatory	Type	Description
			• DEFAULT_5XX: Another 5XX error occurred. • THIRD_AUTH_FAILURE: Third-party authentication failed. • THIRD_AUTH_IDENTITY_FAILURE: The identity source of the third-party authorizer is missing or invalid. • THIRD_AUTH_CONF_FAILURE: A third-party authorizer error has occurred. For example, communication failed or an error response was returned. • ORCHESTRATION_PARAMETER_NOT_FOUND: Parameter orchestration failed. No input parameter is found in the request. • ORCHESTRATION_FAILURE: Parameter orchestration failed. No orchestration rule to match.

Request Parameters

Table 4-1162 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1163 Request body parameters

Parameter	Mandatory	Type	Description
status	No	Integer	HTTP status code of the response. The value ranges from 200 to 599, but cannot be 444.
body	No	String	Response body template.
headers	No	Array of ResponseInfoHeader objects	Custom response header. Array Length: 0 - 10

Table 4-1164 ResponseInfoHeader

Parameter	Mandatory	Type	Description
key	No	String	Key of the custom group response header, which can contain 1 to 128 characters of letters, digits, and hyphens (-).
value	No	String	Value of the custom group response header, which is a string of 1 to 1,024 characters. Minimum: 1 Maximum: 1024

Response Parameters

Status code: 200

Table 4-1165 Response body parameters

Parameter	Type	Description
{User defined key}	Map<String, ResponseInfoResp >	

Table 4-1166 ResponseInfoResp

Parameter	Type	Description
status	Integer	HTTP status code of the response. The value ranges from 200 to 599, but cannot be 444.
body	String	Response body template.
headers	Array of ResponseInfoHeader objects	Custom response header. Array Length: 0 - 10
default	Boolean	Indicates whether the response is the default response.

Table 4-1167 ResponseInfoHeader

Parameter	Type	Description
key	String	Key of the custom group response header, which can contain 1 to 128 characters of letters, digits, and hyphens (-).
value	String	Value of the custom group response header, which is a string of 1 to 1,024 characters. Minimum: 1 Maximum: 1024

Status code: 400**Table 4-1168** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1169** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 403**Table 4-1170** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1171** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1172** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Modifying the response of an error type defined for an API group

```
{
  "body": "body: \"{\\\"error_code\\\":\\\"$context.error.code\\\",\\\"error_msg\\\":\\\"$context.error.message\\\",\\\"request_id\\\":\\\"$context.requestId\\\"}\"",
  "status": 403
}
```

Example Responses

Status code: 200

OK

```
{
  "ACCESS_DENIED" : {
    "body" : "{\"error_code\":\"$context.error.code\",\"error_msg\":\"$context.error.message\",\"request_id\":\"$context.requestId\"}",
    "default" : true,
    "status" : 403
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:group_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3001",
  "error_msg" : "API group c77f5e81d9cb4424bf704ef2b0ac7600 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized

Status Code	Description
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.19.7 Deleting the Response of an Error Type

Function

This API is used to delete the response of an error type defined for an API group. After the response is deleted, the default response of the error type is used.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}/{response_type}

Table 4-1173 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.
response_id	Yes	String	Response ID.

Parameter	Mandatory	Type	Description
response_type	Yes	String	Error type. Options: • AUTH_FAILURE: IAM or app authentication failed. • AUTH_HEADER_MISSING: The identity source is missing. • AUTHORIZER_FAILURE: Custom authentication failed. • AUTHORIZER_CONF_FAILURE: A custom authorizer error has occurred. For example, communication failed or an error response was returned. • AUTHORIZER_IDENTITY_FAILURE: The identity source of the frontend custom authorizer is missing or invalid. • BACKEND_UNAVAILABLE: The backend is unavailable due to communication error. • BACKEND_TIMEOUT: Communication with the backend timed out. • THROTTLED: The request was rejected due to throttling. • UNAUTHORIZED: The credential you use is not authorized to call the API. • ACCESS_DENIED: Access denied. For example, the access control policy is triggered or an attack is detected. • NOT_FOUND: No API is matched. • REQUEST_PARAMETERS_FAILURE: Invalid request parameter or unsupported HTTP method. • DEFAULT_4XX: Another 4XX error occurred.

Parameter	Mandatory	Type	Description
			• DEFAULT_5XX: Another 5XX error occurred. • THIRD_AUTH_FAILURE: Third-party authentication failed. • THIRD_AUTH_IDENTITY_FAILURE: The identity source of the third-party authorizer is missing or invalid. • THIRD_AUTH_CONF_FAILURE: A third-party authorizer error has occurred. For example, communication failed or an error response was returned. • ORCHESTRATION_PARAMETER_NOT_FOUND: Parameter orchestration failed. No input parameter is found in the request. • ORCHESTRATION_FAILURE: Parameter orchestration failed. No orchestration rule to match.

Request Parameters

Table 4-1174 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-1175 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1176** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1177** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1178** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1179** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:group_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3001",
  "error_msg" : "API group c77f5e81d9cb4424bf704ef2b0ac7600 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.19.8 Querying Group Responses

Function

This API is used to query the responses of an API group.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses

Table 4-1180 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.

Table 4-1181 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20

Request Parameters

Table 4-1182 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1183 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
responses	Array of ResponsesInfo objects	Response list.

Table 4-1184 ResponsesInfo

Parameter	Type	Description
name	String	Response name.

Parameter	Type	Description
responses	Map<String, ResponseInfoResp >	Response type definition. key indicates the error type. Options of key: • AUTH_FAILURE: Authentication failed. • AUTH_HEADER_MISSING: The identity source is missing. • AUTHORIZER_FAILURE: Custom authentication failed. • AUTHORIZER_CONF_FAILURE: Custom authorizer error. • AUTHORIZER_IDENTITY_FAILURE: The identity source of the custom authorizer is invalid. • BACKEND_UNAVAILABLE: The backend is unavailable. • BACKEND_TIMEOUT: Backend timed out. • THROTTLED: The request was rejected due to request throttling. • UNAUTHORIZED: The app you are using has not been authorized to call the API. • ACCESS_DENIED: Access denied. • NOT_FOUND: No API is found. • REQUEST_PARAMETERS_FAILURE: Invalid request parameter. • DEFAULT_4XX: Default 4XX error occurred. • DEFAULT_5XX: Default 5XX error occurred. • THIRD_AUTH_FAILURE: Third-party authentication failed. • THIRD_AUTH_IDENTITY_FAILURE: Identity source of the third-party authorizer is invalid. • THIRD_AUTH_CONF_FAILURE: Third-party authorizer configuration error. • ORCHESTRATION_PARAMETER_NOT_FOUND: No parameters are input to match the parameter orchestration rule, causing orchestration failure. • ORCHESTRATION_FAILURE: Input parameters cannot match

Parameter	Type	Description
		orchestration rules, causing orchestration failure. Each error type is in JSON format.
id	String	Response ID.
default	Boolean	Indicates whether the group response is the default response.
create_time	String	Creation time.
update_time	String	Update time.

Table 4-1185 ResponseInfoResp

Parameter	Type	Description
status	Integer	HTTP status code of the response. The value ranges from 200 to 599, but cannot be 444.
body	String	Response body template.
headers	Array of ResponseInfoHeader objects	Custom response header. Array Length: 0 - 10
default	Boolean	Indicates whether the response is the default response.

Table 4-1186 ResponseInfoHeader

Parameter	Type	Description
key	String	Key of the custom group response header, which can contain 1 to 128 characters of letters, digits, and hyphens (-).
value	String	Value of the custom group response header, which is a string of 1 to 1,024 characters. Minimum: 1 Maximum: 1024

Status code: 400

Table 4-1187 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1188** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1189** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1190** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1191** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 2,
  "size" : 2,
  "responses" : [ {
    "create_time" : "2020-08-12T06:52:02Z",
    "default" : false,
    "id" : "e839b367e10f4ab19d1c5008e476b83a",
    "name" : "response_demo",
    "update_time" : "2020-08-12T06:52:02Z"
  }, {
    "create_time" : "2020-07-31T11:39:23Z",
    "default" : true,
    "id" : "ed8e8c52ab0e4a1c9c809268e5002e64",
    "name" : "default",
    "update_time" : "2020-07-31T11:39:23Z"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:group_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3001",
  "error_msg" : "API group c77f5e81d9cb4424bf704ef2b0ac7600 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.20 Tag Management

4.20.1 Querying API Tags

Function

This API is used to query tags of an API.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/tags

Table 4-1192 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1193 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20

Request Parameters

Table 4-1194 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1195 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
tags	Array of strings	Tag list.

Status code: 400**Table 4-1196** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1197** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1198** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1199 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1200** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 2,
  "size" : 2,
  "tags" : [ "webApi", "functionApi" ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
}
```

```
{
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.21 Gateway Feature Management

4.21.1 Configuring a Feature for a Gateway

Function

This API is used to configure a feature for a gateway.

For details about the supported features and configuration examples, see "Appendix" > "Supported Features" in this document.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/features

Table 4-1201 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1202 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1203 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Feature name. Minimum: 1 Maximum: 64
enable	Yes	Boolean	Indicates whether to enable the feature.
config	No	String	Parameter configuration.

Response Parameters

Status code: 201

Table 4-1204 Response body parameters

Parameter	Type	Description
id	String	Feature ID.
name	String	Feature name. Minimum: 1 Maximum: 64
enable	Boolean	Indicates whether to enable the feature.
config	String	Parameter configuration.
instance_id	String	Gateway ID.
update_time	String	Feature update time.

Status code: 400**Table 4-1205** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1206** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1207** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1208** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1209** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Enabling the app_api_key switch

```
{
  "name" : "app_api_key",
  "config" : "on",
  "enable" : true
}
```

Example Responses

Status code: 201

Created

```
{
  "config" : "on",
  "enable" : true,
  "id" : "db9a9260cd3e4a16a9b5747a65d3ffaa",
  "instance_id" : "eddc4d25480b4cd6b512f270a1b8b341",
  "name" : "app_api_key",
  "update_time" : "2020-08-24T01:17:31.041984021Z"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2000",
  "error_msg" : "unrecognized feature app-api-key"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.21.2 Querying Gateway Features

Function

This API is used to query the features of a gateway. If a gateway does not support the features listed in the following table, contact technical support to upgrade the gateway.

For details about the supported features and configuration examples, see "Appendix" > "Supported Features" in this document.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/features

Table 4-1210 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1211 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20

Request Parameters

Table 4-1212 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1213 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
features	Array of FeatureInfo objects	Feature list.

Table 4-1214 FeatureInfo

Parameter	Type	Description
id	String	Feature ID.
name	String	Feature name. Minimum: 1 Maximum: 64
enable	Boolean	Indicates whether to enable the feature.
config	String	Parameter configuration.
instance_id	String	Gateway ID.
update_time	String	Feature update time.

Status code: 400

Table 4-1215 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1216** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1217** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1218** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1219** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "features" : [ {
    "config" : "on",
    "enable" : true,
    "id" : "db9a9260cd3e4a16a9b5747a65d3ffaa",
    "instance_id" : "eddc4d25480b4cd6b512f270a1b8b341",
    "name" : "app_api_key",
    "update_time" : "2020-08-24T01:17:31.041984Z"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```


Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.21.3 Querying the Supported Features of a Gateway

Function

This API is used to query the supported features of a gateway.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/instance-features

Table 4-1220 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1221 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20

Request Parameters

Table 4-1222 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1223 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.

Parameter	Type	Description
features	Array of strings	Supported features: • "resize_huge_flavor" • "health_check_in_instance_etcd" • "shubao_support_add_node" • "upgrade_uninterrupted" • "sm_cipher_type" Features not displayed in the list are not supported by the gateway.

Status code: 401**Table 4-1224** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1225** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1226** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 3,
  "size" : 3,
  "features" : [ "health_check_in_instance_etcd", "shubao_support_add_node", "resize_huge_flavor" ]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.22 Configuration Management

4.22.1 Querying Resource Configurations of a Gateway

Function

This API is used to query the resource configurations and usage of a gateway.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/project/configs

Table 4-1227 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1228 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20

Request Parameters

Table 4-1229 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1230 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
configs	Array of Config objects	Quota list.

Table 4-1231 Config

Parameter	Type	Description
config_id	String	Quota ID.
config_name	String	Quota name.
config_value	String	Quota value. It indicates the value of the quota for the current gateway.
config_time	String	Time when the quota is created.

Parameter	Type	Description
remark	String	Quota description. • API_NUM_LIMIT: Maximum number of APIs you can create. • APP_NUM_LIMIT: Maximum number of apps you can create. • APIGROUP_NUM_LIMIT: Maximum number of API groups you can create. • ENVIRONMENT_NUM_LIMIT: Maximum number of environments you can create. • VARIABLE_NUM_LIMIT: Maximum number of environment variables you can create for an API group. • SIGN_NUM_LIMIT: Maximum number of signature keys you can create. • THROTTLE_NUM_LIMIT: Maximum number of request throttling policies you can create. • APIGROUP_DOMAIN_NUM_LIMIT: Maximum number of custom domain names you can bind to an API group. • API_VERSION_NUM_LIMIT: Maximum number of versions you can retain for an API. • VPC_NUM_LIMIT: Maximum number of VPC channels you can create. • VPC_INSTANCE_NUM_LIMIT: Maximum number of cloud servers you can associate with a VPC channel. • API_PARAM_NUM_LIMIT: Maximum number of parameters you can configure for an API. • API_USER_CALL_LIMIT: Maximum number of times an API can be called within a specific period. • ACL_NUM_LIMIT: Maximum number of access control policies you can create. • APP_THROTTLE_LIMIT: Maximum number of excluded apps allowed for a request throttling policy.

Parameter	Type	Description
		• USER_THROTTLE_LIMIT: Maximum number of excluded tenants allowed for a request throttling policy. • API_NUM_LIMIT_PER_GROUP: Maximum number of APIs you can create for an API group. • API_POLICY_NUM_LIMIT: Maximum number of policy backends you can configure for an API. • API_CONDITION_NUM_LIMIT: Maximum number of conditions you can configure for a policy backend. • SL_DOMAIN_CALL_LIMIT: Maximum number of requests that can be sent to a subdomain name within a specific period. • ELB_SWITCH: Whether to enable ELB channels. • AUTHORIZER_NUM_LIMIT: Maximum number of custom authorizers you can create. • AUTHORIZER_IDENTITY_NUM_LIMIT: Maximum number of identity sources you can configure for a custom authorizer. • APP_CODE_NUM_LIMIT: Maximum number of AppCodes you can create for an app. • REGION_MANAGER_WHITELIST_SERVICES: Whitelist of services that are not verified by the region manager. • API_SWAGGER_NUM_LIMIT: Maximum number of Swagger files you can bind to an API group. • API_TAG_NUM_LIMIT: Maximum number of tags you can configure for an API. • LTS_SWITCH: Whether to enable LTS log reporting. • APP_KEY_SECRET_SWITCH: Whether to enable AppKey and AppSecret customization. 1: enable; 2: disable.

Parameter	Type	Description
		• RESPONSE_NUM_LIMIT: Maximum number of responses you can create for an API group. • CONFIG_NUM_LIMIT_PER_APP: Maximum number of configuration items you can set for an app. • BACKEND_TOKEN_ALLOW_SWITCH: Whether to allow tenants to transparently transmit tokens to the backend. 1: allow; 2: disallow. • APP_TOKEN_SWITCH: Whether to enable AppTokens. • API_DESIGNER_SWITCH: Whether to enable the API designer. 1: enable; 2: disable. • APP_API_KEY_SWITCH: Whether to enable APP_API_KEY authentication. • APP_BASIC_SWITCH: Whether to enable APP_BASIC authentication. • APP_JWT_SWITCH: Whether to enable APP_JWT authentication. • APP_ROUTE_SWITCH: Whether to enable app routes. • PUBLIC_KEY_SWITCH: Whether to enable PUBLIC_KEY backend authentication. • APP_SECRET_SWITCH: Whether to enable APP_SECRET authentication. • CASCADE_SWITCH: Whether to enable cascaded gateways. • IS_INIT_API_PATH_HASH: Whether API path hashing has been performed.
used	Long	Used quota of the gateway.

Status code: 400

Table 4-1232 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1233** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1234** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1235** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1236** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "total" : 43,
  "size" : 2,
  "configs" : [ {
    "config_id" : "9",
    "config_name" : "API_VERSION_NUM_LIMIT",
    "config_value" : "10",
    "config_time" : "2019-02-12T19:42:19.914989Z",
    "remark" : "xxx",
    "used" : 0
  }, {
    "config_id" : "8",
    "config_name" : "APIGROUP_DOMAIN_NUM_LIMIT",
    "config_value" : "5",
    "config_time" : "2019-02-12T19:42:19.914989Z",
    "remark" : "xxx",
    "used" : 0
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:eddc4d25480b4cd6b512f270a1b8b341"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.22.2 Querying Gateway Configurations

Function

This API is used to query the gateway configurations.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instance/configs

Table 4-1237 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Table 4-1238 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20

Request Parameters

Table 4-1239 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1240 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
configs	Array of InstanceConfig objects	Quota list.

Table 4-1241 InstanceConfig

Parameter	Type	Description
config_id	String	Quota ID.
config_name	String	Quota name.
config_value	String	Quota value. It indicates the value of the quota for the current gateway.
config_time	String	Time when the quota is created.
remark	String	Quota description. INSTANCE_NUM_LIMIT: Maximum number of gateways that you can create.

Status code: 400**Table 4-1242** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1243** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1244** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1245** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "total" : 1,
  "size" : 1,
  "configs" : [ {
    "config_id" : "1",
    "config_name" : "INSTANCE_NUM_LIMIT",
    "config_value" : "5",
    "config_time" : 1597981093255,
    "remark" : "xxx"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23 Gateway Management

4.23.1 Creating a Dedicated Gateway (Pay-Per-Use)

Function

This API is used to create a pay-per-use dedicated gateway.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances

Table 4-1246 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Request Parameters

Table 4-1247 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1248 Request body parameters

Parameter	Mandatory	Type	Description
description	No	String	Gateway description. The value can contain up to 255 characters except > and <.
maintain_begin	No	String	Start time of the maintenance time window. It must be in the format "xx:00:00". The value of xx can be 02, 06, 10, 14, 18, or 22. During the maintenance time period, O&M personnel perform maintenance on the gateway. During this period, services can still be used, but occasionally there may be temporary interruptions. Scheduled maintenance occurs infrequently (typically once every several months).
maintain_end	No	String	End time of the maintenance time window. It must be in the format "xx:00:00". There is a 4-hour difference between the start time and end time. During the maintenance time period, O&M personnel perform maintenance on the gateway. During this period, services can still be used, but occasionally there may be temporary interruptions. Scheduled maintenance occurs infrequently (typically once every several months).

Parameter	Mandatory	Type	Description
instance_name	Yes	String	Gateway name. Enter 3 to 64 characters, starting with a letter. Only letters, digits, hyphens (-), and underscores (_) are allowed. Minimum: 3 Maximum: 64
instance_id	No	String	Gateway ID, which will be automatically generated if you do not specify this parameter.
spec_id	Yes	String	Gateway edition. Options: • BASIC • PROFESSIONAL • ENTERPRISE • PLATINUM • BASIC_IPV6 • PROFESSIONAL_IPV6 • ENTERPRISE_IPV6 • PLATINUM_IPV6 • PLATINUM_X2 • PLATINUM_X3 • PLATINUM_X4 • PLATINUM_X5 • PLATINUM_X6 • PLATINUM_X7 • PLATINUM_X8 Platinum 2–8 are available only in certain regions.
vpc_id	Yes	String	VPC ID. You can obtain it in either of the following ways: • Method 1: Log in to the VPC console, and click the name of a VPC to view the VPC ID on the displayed details page. • Method 2: Call the corresponding VPC API. For details, see section "Querying VPCs" in the VPC API Reference.

Parameter	Mandatory	Type	Description
subnet_id	Yes	String	Subnet network ID. You can obtain it in either of the following ways: • Method 1: Log in to the VPC console and click the target subnet on the Subnets page. You can view the network ID on the displayed page. • Method 2: Call the corresponding VPC API. For details, see section "Querying Subnets" in the VPC API Reference.
security_group_id	Yes	String	ID of the security group to which the gateway belongs. You can obtain it in either of the following ways: • Method 1: Log in to the VPC console. Choose Access Control > Security Groups in the navigation pane. On the Security Groups page, click the target security group. Then view the security group ID on the displayed page. • Method 2: Call the corresponding VPC API. For details, see section "Querying Security Groups" in the VPC API Reference.

Parameter	Mandatory	Type	Description
eip_id	No	String	EIP ID. This parameter is required if public access is enabled for the gateway and loadbalancer_provider is set to lvs. After you bind an EIP to the gateway, users can access APIs in the gateway from public networks using the EIP. To obtain an EIP ID, log in to the VPC console, and choose "Elastic IP and Bandwidth" > "EIPs" in the navigation pane. Click the name of the target EIP, and view the EIP ID on the displayed page.
enterprise_project_id	No	String	Enterprise project ID. This parameter is required for an enterprise account. You can obtain it in either of the following ways: • Method 1: Log in to the Enterprise Project Management page, click the name of the target enterprise project, and view the project ID on the displayed page. • Method 2: Call the corresponding project management API. For details, see section "Querying the Enterprise Project List" in the Enterprise Management API Reference.

Parameter	Mandatory	Type	Description
available_zone_ids	Yes	Array of strings	AZs. An AZ is a physical region where resources use independent power supply and networks. AZs are physically isolated but interconnected through an internal network. To enhance application availability, create gateways in different AZs. To obtain AZ information, call the API used to query AZs.
bandwidth_size	No	Integer	Outbound access bandwidth. This parameter is required if public outbound access is enabled for the gateway. After you configure the bandwidth for the gateway, users can access resources on public networks. Default: 5
bandwidth_charging_mode	No	String	Billing type of the public outbound access bandwidth. This parameter is required if public outbound access is enabled for the gateway. bandwidth: billed by bandwidth Default: bandwidth
ipv6_enable	No	Boolean	Indicates whether public access with an IPv6 address is supported. Currently, IPv6 addresses are supported only in certain regions.

Parameter	Mandatory	Type	Description
loadbalancer_provider	No	String	Type of the load balancer used by the gateway. • This field is discarded. Whether to use ELB or LVS is determined by the region of your gateway. For details, see section "Notes and Constraints" in the API Gateway Service Overview. • lvs: Linux VM • elb: Elastic Load Balancer (available only in certain regions) Default: lvs
tags	No	Array of TmsKeyValue objects	Tags. A maximum of 20 tags can be created for a gateway. Array Length: 0 - 20
vpcep_service_name	No	String	Name of a VPC endpoint service. It can contain max. 16 characters, including letters, digits, hyphens (-), and underscores. If this parameter is not specified, the system automatically generates a name in the "{region}.apig.{service_id}" format. If this parameter is specified, the system automatically generates a name in the "{region}. {vpcep_service_name}. {service_id}" format. After the gateway is created, you can modify this name on the Gateways > VPC Endpoints page.

Parameter	Mandatory	Type	Description
ingress_bandwidth_size	No	Integer	Public inbound access bandwidth. This parameter is required if public inbound access is enabled for the gateway and loadbalancer_provider is set to elb. After you bind an EIP to the gateway, users can access APIs in the gateway from public networks using the EIP. Default: 5
ingress_bandwidth_charging_mode	No	String	Billing type of the public inbound access bandwidth. This parameter is required if public inbound access is enabled for the gateway and loadbalancer_provider is set to elb. bandwidth: billed by bandwidth Default: bandwidth

Table 4-1249 TmsKeyValue

Parameter	Mandatory	Type	Description
key	No	String	Key. Include UTF-8 letters, digits, spaces, or special characters (._:=-@). Do not start with _sys_ because it is a system label. Minimum: 1 Maximum: 128
value	No	String	Value. You can enter letters, digits, and spaces or other special characters (._:=-@) in UTF-8 format. Minimum: 0 Maximum: 255

Response Parameters

Status code: 202

Table 4-1250 Response body parameters

Parameter	Type	Description
instance_id	String	Gateway ID.
message	String	Information about the gateway creation task.
job_id	String	Task ID.

Status code: 400

Table 4-1251 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1252 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1253 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1254 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1255** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Creating a gateway with network and security group configurations

```
{
  "available_zone_ids" : [ "xx-xxx-7b", "xx-xxx-7a" ],
  "bandwidth_size" : 5,
  "description" : "test create instance",
  "eip_id" : "41f961ab-2bdd-4ca7-9b59-cfc4fcef10c9",
  "enterprise_project_id" : "0",
  "instance_name" : "apig-demo",
  "maintain_begin" : "22:00:00",
  "maintain_end" : "02:00:00",
  "security_group_id" : "36d0ec18-bd10-4da7-86f3-ad7a5ddc55d7",
  "spec_id" : "PROFESSIONAL",
  "subnet_id" : "a938121c-11c4-4c91-b983-bc9acd347bb5",
  "vpc_id" : "0957108c-257c-4ce0-9e93-527d279ce763"
}
```

Example Responses

Status code: 202

Accepted

```
{
  "instance_id" : "6a7d71827fd54572b1f31aa9548fcc81",
  "message" : "JOB_ASSIGNED_FOR_PROVISIONING_0003I:The job JOB-bdb370eb6f4c4c73b61b95a9da38beb5 has been assigned to the instance 6a7d71827fd54572b1f31aa9548fcc81 for running provisioning.",
  "job_id" : "JOB-edbac2355fb7433e98f173ea2e452e2d"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIC.7211",
  "error_msg" : "Parameter value does not match the rules, parameter name[maintainBegin]"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7301",
  "error_msg" : "Instance spec not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
202	Accepted
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.23.2 Querying Dedicated Gateway Details

Function

This API is used to query the details of a dedicated gateway.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}

Table 4-1256 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1257 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1258 Response body parameters

Parameter	Type	Description
id	String	Gateway ID.

Parameter	Type	Description
project_id	String	ID of the tenant to which the gateway belongs.
instance_name	String	Gateway name.

Parameter	Type	Description
status	String	Instance status: • Creating: The instance is being created. • CreateSuccess: The instance is created successfully. • CreateFail: The instance fails to be created. • Initing: The instance is being initialized. • Registering: The instance is being registered. • Running: The instance is running. • InitingFailed: The instance fails to be initialized. • RegisterFailed: The instance fails to be registered. • Installing: The instance is being installed. • InstallFailed: The instance fails to be installed. • Updating: The instance is being upgraded. • UpdateFailed: The instance fails to be upgraded. • Rollbacking: The instance is being rolled back. • RollbackSuccess: The instance is rolled back successfully. • RollbackFailed: The instance fails to be rolled back. • Deleting: The instance is being deleted. • DeleteFailed: The instance fails to be deleted. • Unregistering: The instance is being deregistered. • UnRegisterFailed: The instance fails to be deregistered. • CreateTimeout: Creation of the instance times out. • InitTimeout: Initialization of the instance times out. • RegisterTimeout: Registration of the instance times out.

Parameter	Type	Description
		• InstallTimeout: Installation of the instance times out. • UpdateTimeout: Upgrading of the instance times out. • RollbackTimeout: Rollback of the instance times out. • DeleteTimeout: Deletion of the instance times out. • UnregisterTimeout: Deregistration of the instance times out. • Starting: The instance is being started. • Freezing: The instance is being frozen. • Frozen: The instance is frozen. • Restarting: The instance is being restarted. • RestartFail: The instance fails to be restarted. • Unhealthy: The instance is abnormal. • RestartTimeout: Restart of the instance times out. • Resizing: The instance specification is changing. • ResizeFailed: The instance specification fails to be changed. • ResizeTimeout: The instance specification change times out.

Parameter	Type	Description
instance_status	Integer	Instance status ID: • 1: Creating • 2: Created successfully • 3: Creation failed • 4: Initializing • 5: Registering • 6: Running • 7: Initialization failed • 8: Registration failed • 10: Installing • 11: Installation failed • 12: Upgrading • 13: Upgrade failed • 20: Rolling back • 21: Rolled back • 22: Rollback failed • 23: Deleting • 24: Deletion failed • 25: Deregistering • 26: Deregistration failed • 27: Creation timed out • 28: Initialization timed out • 29: Registration timed out • 30: Installation timed out • 31: Upgrade timed out • 32: Rollback timed out • 33: Deletion timed out • 34: Deregistration timed out • 35: Starting • 36: Freezing • 37: Frozen • 38: Restarting • 39: Restart failed • 40: Abnormal • 41: Restart timed out • 42: Changing specification • 43: Specification change failed • 44: Specification change timed out

Parameter	Type	Description
type	String	Gateway type. The default value is apig.
spec	String	Gateway edition. • BASIC • PROFESSIONAL • ENTERPRISE • PLATINUM • BASIC_IPV6 • PROFESSIONAL_IPV6 • ENTERPRISE_IPV6 • PLATINUM_IPV6
create_time	Long	Time when the gateway is created. The time is in the Unix timestamp format.
enterprise_project_id	String	Enterprise project ID. This parameter is required for an enterprise account.
eip_address	String	EIP bound to the gateway.
charging_mode	Integer	Billing mode of the gateway. • 0: pay-per-use • 1: This parameter is not used currently.
cbc_metadata	String	This parameter is not used currently.
loadbalancer_provider	String	Type of the load balancer used by the gateway. • LVS • ELB (available only in certain regions) Default: lvs
cbc_operation_locks	Array of CbcOperationLock objects	Cloud operations restriction lock
description	String	Description about the gateway.

Parameter	Type	Description
vpc_id	String	VPC ID. You can obtain it in either of the following ways: • Method 1: Log in to the VPC console, and click the name of a VPC to view the VPC ID on the displayed details page. • Method 2: Call the corresponding VPC API. For details, see section "Querying VPCs" in the VPC API Reference.
subnet_id	String	Subnet network ID. You can obtain it in either of the following ways: • Method 1: Log in to the VPC console and click the target subnet on the Subnets page. You can view the network ID on the displayed page. • Method 2: Call the corresponding VPC API. For details, see section "Querying Subnets" in the VPC API Reference.
security_group_id	String	ID of the security group to which the gateway belongs. You can obtain it in either of the following ways: • Method 1: Log in to the VPC console. Choose Access Control > Security Groups in the navigation pane. On the Security Groups page, click the target security group. Then view the security group ID on the displayed page. • Method 2: Call the corresponding VPC API. For details, see section "Querying Security Groups" in the VPC API Reference.

Parameter	Type	Description
maintain_begin	String	Start time of the maintenance time window. It must be in the format "xx:00:00". The value of xx can be 02, 06, 10, 14, 18, or 22. During the maintenance time period, the O&M personnel can perform maintenance operations on the gateway. During maintenance, services can still be used, but occasionally there may be temporary service interruptions. Scheduled maintenance occurs infrequently (typically once every several months).
maintain_end	String	End time of the maintenance time window. It must be in the format "xx:00:00". There is a 4-hour difference between the start time and end time. During the maintenance time period, the O&M personnel can perform maintenance operations on the gateway. During maintenance, services can still be used, but occasionally there may be temporary service interruptions. Scheduled maintenance occurs infrequently (typically once every several months).
ingress_ip	String	VPC ingress address.
ingress_ip_v6	String	VPC access address (IPv6).
user_id	String	ID of the account to which the gateway belongs.
nat_eip_ipv6_cidr	String	Public egress address (IPv6). Currently, IPv6 addresses are supported only in certain regions.
eip_ipv6_address	String	EIP (IPv6). Currently, IPv6 addresses are supported only in certain regions.
nat_eip_address	String	IP address for public outbound access.
bandwidth_size	Integer	Outbound access bandwidth.
bandwidth_charging_mode	String	Billing mode of the public outbound access bandwidth.
available_zone_ids	String	AZ.
instance_version	String	Gateway version.

Parameter	Type	Description
virsubnet_id	String	Subnet network ID. Currently, this parameter is not supported.
roma_eip_address	String	ROMA EIP. Currently, this parameter is not supported.
listeners	Object	Listener information. Currently, this parameter is not supported.
supported_features	Array of strings	Supported features.
endpoint_service	EndpointService object	VPC endpoint service details. This parameter will be deprecated. Use endpoint_services instead.
endpoint_services	Array of EndpointService objects	VPC endpoint services.
node_ips	NodeIps object	VPC endpoint ID.
node_ipv6_ips	NodeIps object	IPv6 address of the service node.
public_ipv6_ips	Array of strings	IPv6 address for public outbound access.
publicips	Array of IpDetails objects	Public inbound access addresses.
privateips	Array of IpDetails objects	Private inbound access addresses.
unreliable_ips	Array of strings	List of unreliable gateway inbound access IP addresses, to which the subdomain name of the group is not CNAMEd. The DEFAULT group cannot be accessed directly using the IP address in this list.
enable_fullstack_ipv6	Boolean	Whether the gateway supports full-format IPv6. • true: The gateway supports IPv6 for both inbound and outbound access. • false: Not supported. The gateway supports IPv6 only for inbound access.

Parameter	Type	Description
is_releasable	Boolean	Whether the gateway can be released. - true: The gateway can be released. - false: The gateway cannot be released.
ingress_bandwidth h_charging_mode	String	Billing mode of the public inbound access bandwidth.

Table 4-1259 CbcOperationLock

Parameter	Type	Description
lock_scene	String	Restriction scenarios: - TO_PERIOD_LOCK: This parameter is not supported currently. - SPEC_CHG_LOCK: This parameter is not supported currently.
lock_source_id	String	ID of the object that initiates the restriction

Table 4-1260 EndpointService

Parameter	Type	Description
service_name	String	VPC endpoint service name.
created_at	String	Creation time.

Table 4-1261 NodeIps

Parameter	Type	Description
livedata	Array of strings	LiveData node IP addresses.
shubao	Array of strings	Shubao node IP addresses.

Table 4-1262 IpDetails

Parameter	Type	Description
ip_address	String	IP address.
ipv6_address	String	IPv6 address.

Parameter	Type	Description
bandwidth_size	Integer	Bandwidth.

Status code: 401**Table 4-1263** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1264** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1265** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1266** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "id" : "8dfxxxxxxxxxxxxxxxxxxxx00p",
  "spec" : "BASIC",
  "project_id" : "78xxxxxxxxxxxxxxxxxxxxoi",
  "instance_name" : "apig-demo",
  "status" : "Running",
  "instance_status" : 6,
  "eip_address" : null,
  "type" : null,
  "create_time" : 1635890506328,
  "charging_mode" : 0,
  "enterprise_project_id" : "0",
  "loadbalancer_provider" : "elb",
  "description" : "test create instance",
  "instance_version" : "acc6d368a3cb4d47840380bf62b0ab32",
  "available_zone_ids" : "[xx-xxx-7a, xx-xxx-7b]",
  "user_id" : "e966ff7227ef4df49df7d57aaf00f8ed",
  "vpc_id" : "0402ea19-5457-4032-9d1b-eb48b98f6c66",
  "subnet_id" : "a3bd29e4-d5bc-414c-a79a-1f35ee4ead88",
  "vpc_subnet_id" : "a3bd29e4-d5bc-414c-a79a-1f35ee4ead88",
  "security_group_id" : "4b95a790-5cfc-463d-8de5-42199e55371c",
  "maintain_begin" : "22:00:00",
  "maintain_end" : "02:00:00",
  "ingress_ip" : "192.168.0.152",
  "ingress_ip_v6" : null,
  "nat_eip_address" : "xxx.xxx.xxx.xxx",
  "roma_eip_address" : null,
  "bandwidth_size" : 5,
  "bandwidth_charging_mode" : "bandwidth",
  "nat_eip_ipv6_cidr" : null,
  "eip_ipv6_address" : null,
  "supported_features" : [ "lts", "gateway_responses", "ratelimit", "request_body_size", "backend_timeout",
    "app_token", "app_basic", "app_secret", "multi_auth", "route", "sign_basic", "app_route",
    "backend_client_certificate", "ssl_ciphers", "cors", "app_quota", "app_acl", "real_ip_from_xff",
    "set_resp_headers", "vpc_backup", "throttle_strategy", "watch_instance", "sign_aes",
    "mock_status_code_and_header", "backend_retry_count", "custom_log", "real_ip_header_getter",
    "policy_sys_param", "vpc_name_modifiable", "breaker", "default_group_host_trustlist" ],
  "node_ips" : {
    "livedata" : [ ],
    "shubao" : [ "192.168.0.123", "192.168.0.114" ]
  },
  "endpoint_service" : null,
  "endpoint_services" : [ {
    "service_name" : "xx-xxx-7a.apig.20bc4a91-1542-43s2-a278-b1e49c0hh6f9",
    "created_at" : "2021-8-03 06:04:43"
  } ],
  "publicips" : [ {
    "ip_address" : "xxx.xxx.xxx.xxx",
    "ipv6_address" : "xxx:xxx:xxx:xxx:xxx:xxx:xxx:2b8",
    "bandwidth_size" : 5
  } ],
  "privateips" : [ {
    "ip_address" : "xxx.xxx.xxx.xxx",
    "ipv6_address" : "xxx:xxx:xxx:xxx:xxx:xxx:xxx:2b8",
    "bandwidth_size" : 5
  } ],
  "ingress_bandwidth_charging_mode" : "bandwidth",
  "cbc_operation_locks" : [ {
```

```
{
  "lock_scene" : "TO_PERIOD_LOCK",
  "lock_source_id" : "CxxxxxxxxxM"
},
"public_ipv6_ips" : [ "xxx:xxx:xxx:xxx:xxx:xxx:xxx:2b83", "xxx:xxx:xxx:xxx:xxx:xxx:xxx:6fee" ],
"node_ipv6_ips" : {
  "livedata" : [ ],
  "shubao" : [ "xxx:xxx:xxx:xxx:xxx:xxx:xxx:2b81", "xxx:xxx:xxx:xxx:xxx:xxx:xxx:2b84" ]
},
"enable_fullstack_ipv6" : true,
"unreliable_ips" : [ "192.xx.xxx.xxx" ]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7302",
  "error_msg" : "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23.3 Updating a Dedicated Gateway

Function

This API is used to update a dedicated gateway.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}

Table 4-1267 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1268 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1269 Request body parameters

Parameter	Mandatory	Type	Description
description	No	String	Gateway description. The value can contain up to 255 characters except > and <.
maintain_begin	No	String	Start time of the maintenance time window. It must be in the format "xx:00:00". The value of xx can be 02, 06, 10, 14, 18, or 22. During the maintenance time period, O&M personnel perform maintenance on the gateway. During this period, services can still be used, but occasionally there may be temporary interruptions. Scheduled maintenance occurs infrequently (typically once every several months).
maintain_end	No	String	End time of the maintenance time window. It must be in the format "xx:00:00". There is a 4-hour difference between the start time and end time. During the maintenance time period, O&M personnel perform maintenance on the gateway. During this period, services can still be used, but occasionally there may be temporary interruptions. Scheduled maintenance occurs infrequently (typically once every several months).
instance_name	No	String	Gateway name. Enter 3 to 64 characters, starting with a letter. Only letters, digits, hyphens (-), and underscores (_) are allowed. Minimum: 3 Maximum: 64

Parameter	Mandatory	Type	Description
security_group_id	No	String	Security group to which the gateway belongs. You can obtain it in either of the following ways: • Method 1: Log in to the VPC console. Choose Access Control > Security Groups in the navigation pane. On the Security Groups page, click the target security group. Then view the security group ID on the displayed page. • Method 2: Call the corresponding VPC API. For details, see section "Querying Security Groups" in the VPC API Reference.
vpcep_service_name	No	String	Name of a VPC endpoint service. It can contain max. 16 characters, including letters, digits, hyphens (-), and underscores. If this parameter is not specified, the system automatically generates a name in the "{region}. {service_id}" format. If this parameter is specified, the system automatically generates a name in the "{region}. {vpcep_service_name}. {service_id}" format.

Response Parameters

Status code: 200

Table 4-1270 Response body parameters

Parameter	Type	Description
id	String	Gateway ID.

Parameter	Type	Description
project_id	String	ID of the tenant to which the gateway belongs.
instance_name	String	Gateway name.

Parameter	Type	Description
status	String	Instance status: • Creating: The instance is being created. • CreateSuccess: The instance is created successfully. • CreateFail: The instance fails to be created. • Initing: The instance is being initialized. • Registering: The instance is being registered. • Running: The instance is running. • InitingFailed: The instance fails to be initialized. • RegisterFailed: The instance fails to be registered. • Installing: The instance is being installed. • InstallFailed: The instance fails to be installed. • Updating: The instance is being upgraded. • UpdateFailed: The instance fails to be upgraded. • Rollbacking: The instance is being rolled back. • RollbackSuccess: The instance is rolled back successfully. • RollbackFailed: The instance fails to be rolled back. • Deleting: The instance is being deleted. • DeleteFailed: The instance fails to be deleted. • Unregistering: The instance is being deregistered. • UnRegisterFailed: The instance fails to be deregistered. • CreateTimeout: Creation of the instance times out. • InitTimeout: Initialization of the instance times out. • RegisterTimeout: Registration of the instance times out.

Parameter	Type	Description
		• InstallTimeout: Installation of the instance times out. • UpdateTimeout: Upgrading of the instance times out. • RollbackTimeout: Rollback of the instance times out. • DeleteTimeout: Deletion of the instance times out. • UnregisterTimeout: Deregistration of the instance times out. • Starting: The instance is being started. • Freezing: The instance is being frozen. • Frozen: The instance is frozen. • Restarting: The instance is being restarted. • RestartFail: The instance fails to be restarted. • Unhealthy: The instance is abnormal. • RestartTimeout: Restart of the instance times out. • Resizing: The instance specification is changing. • ResizeFailed: The instance specification fails to be changed. • ResizeTimeout: The instance specification change times out.

Parameter	Type	Description
instance_status	Integer	Instance status ID: • 1: Creating • 2: Created successfully • 3: Creation failed • 4: Initializing • 5: Registering • 6: Running • 7: Initialization failed • 8: Registration failed • 10: Installing • 11: Installation failed • 12: Upgrading • 13: Upgrade failed • 20: Rolling back • 21: Rolled back • 22: Rollback failed • 23: Deleting • 24: Deletion failed • 25: Deregistering • 26: Deregistration failed • 27: Creation timed out • 28: Initialization timed out • 29: Registration timed out • 30: Installation timed out • 31: Upgrade timed out • 32: Rollback timed out • 33: Deletion timed out • 34: Deregistration timed out • 35: Starting • 36: Freezing • 37: Frozen • 38: Restarting • 39: Restart failed • 40: Abnormal • 41: Restart timed out • 42: Changing specification • 43: Specification change failed • 44: Specification change timed out

Parameter	Type	Description
type	String	Gateway type. The default value is apig.
spec	String	Gateway edition. • BASIC • PROFESSIONAL • ENTERPRISE • PLATINUM • BASIC_IPV6 • PROFESSIONAL_IPV6 • ENTERPRISE_IPV6 • PLATINUM_IPV6
create_time	Long	Time when the gateway is created. The time is in the Unix timestamp format.
enterprise_project_id	String	Enterprise project ID. This parameter is required for an enterprise account.
eip_address	String	EIP bound to the gateway.
charging_mode	Integer	Billing mode of the gateway. • 0: pay-per-use • 1: This parameter is not used currently.
cbc_metadata	String	This parameter is not used currently.
loadbalancer_provider	String	Type of the load balancer used by the gateway. • LVS • ELB (available only in certain regions) Default: lvs
cbc_operation_locks	Array of CbcOperationLock objects	Cloud operations restriction lock
description	String	Description about the gateway.

Parameter	Type	Description
vpc_id	String	VPC ID. You can obtain it in either of the following ways: • Method 1: Log in to the VPC console, and click the name of a VPC to view the VPC ID on the displayed details page. • Method 2: Call the corresponding VPC API. For details, see section "Querying VPCs" in the VPC API Reference.
subnet_id	String	Subnet network ID. You can obtain it in either of the following ways: • Method 1: Log in to the VPC console and click the target subnet on the Subnets page. You can view the network ID on the displayed page. • Method 2: Call the corresponding VPC API. For details, see section "Querying Subnets" in the VPC API Reference.
security_group_id	String	ID of the security group to which the gateway belongs. You can obtain it in either of the following ways: • Method 1: Log in to the VPC console. Choose Access Control > Security Groups in the navigation pane. On the Security Groups page, click the target security group. Then view the security group ID on the displayed page. • Method 2: Call the corresponding VPC API. For details, see section "Querying Security Groups" in the VPC API Reference.

Parameter	Type	Description
maintain_begin	String	Start time of the maintenance time window. It must be in the format "xx:00:00". The value of xx can be 02, 06, 10, 14, 18, or 22. During the maintenance time period, the O&M personnel can perform maintenance operations on the gateway. During maintenance, services can still be used, but occasionally there may be temporary service interruptions. Scheduled maintenance occurs infrequently (typically once every several months).
maintain_end	String	End time of the maintenance time window. It must be in the format "xx:00:00". There is a 4-hour difference between the start time and end time. During the maintenance time period, the O&M personnel can perform maintenance operations on the gateway. During maintenance, services can still be used, but occasionally there may be temporary service interruptions. Scheduled maintenance occurs infrequently (typically once every several months).
ingress_ip	String	VPC ingress address.
ingress_ip_v6	String	VPC access address (IPv6).
user_id	String	ID of the account to which the gateway belongs.
nat_eip_ipv6_cidr	String	Public egress address (IPv6). Currently, IPv6 addresses are supported only in certain regions.
eip_ipv6_address	String	EIP (IPv6). Currently, IPv6 addresses are supported only in certain regions.
nat_eip_address	String	IP address for public outbound access.
bandwidth_size	Integer	Outbound access bandwidth.
bandwidth_charging_mode	String	Billing mode of the public outbound access bandwidth.
available_zone_ids	String	AZ.
instance_version	String	Gateway version.

Parameter	Type	Description
virsubnet_id	String	Subnet network ID. Currently, this parameter is not supported.
roma_eip_address	String	ROMA EIP. Currently, this parameter is not supported.
listeners	Object	Listener information. Currently, this parameter is not supported.
supported_features	Array of strings	Supported features.
endpoint_service	EndpointService object	VPC endpoint service details. This parameter will be deprecated. Use endpoint_services instead.
endpoint_services	Array of EndpointService objects	VPC endpoint services.
node_ips	NodeIps object	VPC endpoint ID.
node_ipv6_ips	NodeIps object	IPv6 address of the service node.
public_ipv6_ips	Array of strings	IPv6 address for public outbound access.
publicips	Array of IpDetails objects	Public inbound access addresses.
privateips	Array of IpDetails objects	Private inbound access addresses.
unreliable_ips	Array of strings	List of unreliable gateway inbound access IP addresses, to which the subdomain name of the group is not CNAMEd. The DEFAULT group cannot be accessed directly using the IP address in this list.
enable_fullstack_ipv6	Boolean	Whether the gateway supports full-format IPv6. • true: The gateway supports IPv6 for both inbound and outbound access. • false: Not supported. The gateway supports IPv6 only for inbound access.

Parameter	Type	Description
is_releasable	Boolean	Whether the gateway can be released. - true: The gateway can be released. - false: The gateway cannot be released.
ingress_bandwidth h_charging_mode	String	Billing mode of the public inbound access bandwidth.

Table 4-1271 CbcOperationLock

Parameter	Type	Description
lock_scene	String	Restriction scenarios: - TO_PERIOD_LOCK: This parameter is not supported currently. - SPEC_CHG_LOCK: This parameter is not supported currently.
lock_source_id	String	ID of the object that initiates the restriction

Table 4-1272 EndpointService

Parameter	Type	Description
service_name	String	VPC endpoint service name.
created_at	String	Creation time.

Table 4-1273 NodeIps

Parameter	Type	Description
livedata	Array of strings	LiveData node IP addresses.
shubao	Array of strings	Shubao node IP addresses.

Table 4-1274 IpDetails

Parameter	Type	Description
ip_address	String	IP address.
ipv6_address	String	IPv6 address.

Parameter	Type	Description
bandwidth_size	Integer	Bandwidth.

Status code: 400**Table 4-1275** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1276** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1277** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1278** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1279 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Modifying a gateway

```
{
  "description" : "test create instance",
  "instance_name" : "apig-demo"
}
```

Example Responses

Status code: 200

OK

```
{
  "available_zone_ids" : "[xx-xxx-7a, xx-xxx-7b]",
  "bandwidth_size" : 5,
  "description" : "test create instance",
  "enterprise_project_id" : "0",
  "instance_name" : "apig-demo",
  "maintain_begin" : "22:00:00",
  "maintain_end" : "02:00:00",
  "security_group_id" : "36d0ec18-bd10-4da7-86f3-ad7a5ddc55d7",
  "spec" : "PROFESSIONAL",
  "subnet_id" : "a938121c-11c4-4c91-b983-bc9acd347bb5",
  "vpc_id" : "0957108c-257c-4ce0-9e93-527d279ce763",
  "enable_fullstack_ipv6" : true,
  "unreliable_ips" : [ "192.xx.xxx.xxx" ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIC.7211",
  "error_msg" : "Parameter value does not match the rules, parameter name[maintainBegin]"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
}
```

```
{
  "error_msg": "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIC.7302",
  "error_msg": "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIC.9000",
  "error_msg": "Failed to request internal service"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23.4 Querying the Creation Progress of a Dedicated Gateway

Function

This API is used to query the creation progress of a dedicated gateway.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/progress

Table 4-1280 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1281 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1282 Response body parameters

Parameter	Type	Description
progress	Integer	Gateway creation progress. Unit: %
status	String	Gateway creation status. • creating • success • failed
error_code	String	Error code.
error_msg	String	Error message.
start_time	Long	Time when the gateway creation starts. The time is in the Unix timestamp format.

Parameter	Type	Description
end_time	Long	Time when the gateway creation is completed. The time is in the Unix timestamp format.

Status code: 401**Table 4-1283** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1284** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1285** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1286** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

- Gateway created.

```
{
  "end_time" : 1597390224911,
  "error_code" : null,
  "error_msg" : null,
  "progress" : 100,
  "start_time" : 1597389901161,
  "status" : "success"
}
```

- Gateway is being created.

```
{
  "end_time" : 1597390224911,
  "error_code" : null,
  "error_msg" : null,
  "progress" : 50,
  "start_time" : 1597389901161,
  "status" : "creating"
}
```

- Gateway creation failed due to insufficient quota.

```
{
  "end_time" : 1597390224911,
  "error_code" : "APIC.9218",
  "error_msg" : "create failed...",
  "progress" : 0,
  "start_time" : 1597389901161,
  "status" : "failed"
}
```

- Gateway creation failed due to insufficient resources.

```
{
  "end_time" : 1597390224911,
  "error_code" : "APIC.9219",
  "error_msg" : "create failed...",
  "progress" : 0,
  "start_time" : 1597389901161,
  "status" : "failed"
}
```

- Gateway creation failed due to other reasons.

```
{
  "end_time" : 1597390224911,
  "error_code" : "APIC.9206",
  "error_msg" : "create failed...",
  "progress" : 0,
  "start_time" : 1597389901161,
  "status" : "failed"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
}
```

```
{
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIC.7106",
  "error_msg": "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIC.7302",
  "error_msg": "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIC.9000",
  "error_msg": "Failed to request internal service"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23.5 Updating or Binding an EIP to a Dedicated Gateway

Function

This API is used to bind an EIP to a dedicated gateway or update the EIP bound to a dedicated gateway (only available for LVS gateways).

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/eip

Table 4-1287 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1288 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1289 Request body parameters

Parameter	Mandatory	Type	Description
eip_id	No	String	EIP ID.

Response Parameters

Status code: 200

Table 4-1290 Response body parameters

Parameter	Type	Description
eip_id	String	EIP ID.
eip_address	String	EIP.
eip_status	String	EIP status.

Parameter	Type	Description
eip_ipv6_address	String	EIP (IPv6).

Status code: 400**Table 4-1291** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1292** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1293** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1294** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1295 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Binding an EIP to a gateway

```
{
  "eip_id" : "85392b45-685c-4f77-b19a-14ad875b8190"
}
```

Example Responses

Status code: 200

OK

```
{
  "eip_id" : "85392b45-685c-4f77-b19a-14ad875b8190",
  "eip_address" : "xxx.xxx.xxx.xxx",
  "eip_status" : "ACTIVE"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIC.7211",
  "error_msg" : "Parameter value does not match the rules, parameter name[eip_id]"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7302",
  "error_msg" : "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.23.6 Unbinding the EIP of a Dedicated Gateway

Function

This API is used to unbind the EIP of a dedicated gateway.

Calling MethodFor details, see [Calling APIs](#).**URI**

DELETE /v2/{project_id}/apigw/instances/{instance_id}/eip

Table 4-1296 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1297 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

OK

Status code: 401

Table 4-1298 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1299 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1300 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1301** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7302",
  "error_msg" : "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```


Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23.7 Enabling Public Access for a Dedicated Gateway

Function

This API is used to enable public access for a dedicated gateway.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/nat-eip

Table 4-1302 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1303 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1304 Request body parameters

Parameter	Mandatory	Type	Description
bandwidth_size	No	String	Outbound access bandwidth. Unit: Mbit/s
bandwidth_charging_mode	No	String	Billing type of the public outbound access bandwidth. bandwidth: billed by bandwidth Default: bandwidth

Response Parameters

Status code: 200

OK

Status code: 400

Table 4-1305 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1306 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1307** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1308** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1309** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Enabling public access for a gateway

```
{
  "bandwidth_size" : "5",
  "bandwidth_charging_mode" : "bandwidth"
}
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIC.9210",
  "error_msg" : "create cloud nat eip failed"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7302",
  "error_msg" : "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23.8 Updating the Outbound Access Bandwidth of a Dedicated Gateway

Function

This API is used to update the outbound access bandwidth of a dedicated gateway.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/nat-eip

Table 4-1310 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1311 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1312 Request body parameters

Parameter	Mandatory	Type	Description
bandwidth_size	No	String	Outbound access bandwidth. Unit: Mbit/s
bandwidth_charging_mode	No	String	Billing type of the public outbound access bandwidth. bandwidth: billed by bandwidth Default: bandwidth

Response Parameters

Status code: 200

OK

Status code: 400

Table 4-1313 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1314 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1315 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1316** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1317** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Updating the outbound access bandwidth of a gateway

```
{
  "bandwidth_size" : 5,
  "bandwidth_charging_mode" : "bandwidth"
}
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIC.9211",
  "error_msg" : "update bandwidth size failed"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7302",
  "error_msg" : "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.23.9 Disabling Public Access for a Dedicated Gateway

Function

This API is used to disable public access for a dedicated gateway.

Calling MethodFor details, see [Calling APIs](#).**URI**

DELETE /v2/{project_id}/apigw/instances/{instance_id}/nat-eip

Table 4-1318 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1319 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 401

Table 4-1320 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1321 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 404**Table 4-1322** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1323** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7302",
}
```

```
{
  "error_msg": "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIC.9000",
  "error_msg": "Failed to request internal service"
}
```

Status Codes

Status Code	Description
204	No Content
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23.10 Enabling Public Inbound Access

Function

This API is used to enable public inbound access for a gateway that uses ELB for load balancing.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/ingress-eip

Table 4-1324 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1325 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1326 Request body parameters

Parameter	Mandatory	Type	Description
bandwidth_size	No	Integer	Public inbound access bandwidth. Unit: Mbit/s
bandwidth_charging_mode	No	String	Billing type of the public inbound access bandwidth. bandwidth: billed by bandwidth Default: bandwidth

Response Parameters

Status code: 202

Table 4-1327 Response body parameters

Parameter	Type	Description
instance_id	String	Gateway ID.
message	String	Public access address change task.
job_id	String	Task ID.

Status code: 400**Table 4-1328** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1329** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1330** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1331** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1332** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Example Requests

Enabling public inbound access for a gateway

```
{
  "bandwidth_size" : 5,
  "bandwidth_charging_mode" : "bandwidth"
}
```

Example Responses

Status code: 202

Accepted

```
{
  "instance_id" : "6a7d71827fd54572b1f31aa9548fcc81",
  "message" : "JOB_ASSIGNED_FOR_UPDATE_00771:The job JOB-a7c1241c33334490a3fdcd11102bcbda is assigned to the instance 6a7d71827fd54572b1f31aa9548fcc81 for running updating",
  "job_id" : "JOB-a7c1241c33334490a3fdcd11102bcbda"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIC.9210",
  "error_msg" : "create cloud nat eip failed"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7302",
  "error_msg" : "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
202	Accepted
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23.11 Updating Public Inbound Access Bandwidth of a Gateway

Function

This API is used to update the public inbound access bandwidth of a gateway that uses ELB for load balancing.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/ingress-eip

Table 4-1333 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1334 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1335 Request body parameters

Parameter	Mandatory	Type	Description
bandwidth_size	No	Integer	Public inbound access bandwidth. Unit: Mbit/s
bandwidth_charging_mode	No	String	Billing type of the public inbound access bandwidth. bandwidth: billed by bandwidth Default: bandwidth

Response Parameters

Status code: 202

Table 4-1336 Response body parameters

Parameter	Type	Description
instance_id	String	Gateway ID.
message	String	Public access address change task.
job_id	String	Task ID.

Status code: 400**Table 4-1337** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1338** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1339** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1340** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1341** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Example Requests

Updating public inbound access bandwidth of a gateway

```
{
  "bandwidth_size" : 5,
  "bandwidth_charging_mode" : "bandwidth"
}
```

Example Responses

Status code: 202

Accepted

```
{
  "instance_id" : "6a7d71827fd54572b1f31aa9548fcc81",
  "message" : "JOB_ASSIGNED_FOR_UPDATE_00771:The job JOB-a7c1241c33334490a3fdcd11102bcbda is assigned to the instance 6a7d71827fd54572b1f31aa9548fcc81 for running updating",
  "job_id" : "JOB-a7c1241c33334490a3fdcd11102bcbda"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIC.9211",
  "error_msg" : "update bandwidth size failed"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7302",
  "error_msg" : "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
202	Accepted
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23.12 Disabling Public Inbound Access for a Gateway

Function

This API is used to disable public inbound access for a gateway that uses ELB for load balancing.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/ingress-eip

Table 4-1342 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1343 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 401

Table 4-1344 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1345 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1346 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1347 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7302",
  "error_msg" : "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
204	No Content
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23.13 Querying AZs

Function

This API is used to query AZs where you can buy gateways.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/available-zones

Table 4-1348 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Request Parameters

Table 4-1349 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1350 Response body parameters

Parameter	Type	Description
available_zones	Array of AvailableZone objects	AZ list.

Table 4-1351 AvailableZone

Parameter	Type	Description
name	String	AZ name.
id	String	Error message.
code	String	AZ code.
port	String	AZ port.
local_name	LocalName object	AZ names.
specs	Map<String, Boolean>	Gateway editions available in the AZ.

Table 4-1352 LocalName

Parameter	Type	Description
en_us	String	AZ name.
zh_cn	String	AZ name.

Status code: 401**Table 4-1353** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1354** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1355** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "available_zones" : [ {
    "code" : "xx-xxx-4a",
    "id" : "effdcbc7d4d64a02aa1fa26b42f56533",
    "local_name" : {
      "en_us" : "AZ1",
      "zh_cn" : "<Name_of_AZ1>"
    },
    "name" : "<Name_of_AZ1>",
    "port" : "8403",
    "specs" : {
      "BASIC" : true,
      "BASIC_IPV6" : false,
```



```
"ENTERPRISE" : true,
"ENTERPRISE_IPV6" : false,
"PLATINUM" : true,
"PLATINUM_IPV6" : false,
"PROFESSIONAL" : true,
"PROFESSIONAL_IPV6" : false,
"TRIAL" : true,
"PLATINUM_X2" : false,
"PLATINUM_X3" : false,
"PLATINUM_X4" : false,
"PLATINUM_X5" : false,
"PLATINUM_X6" : false,
"PLATINUM_X7" : false,
"PLATINUM_X8" : false
}
}, {
  "code" : "xx-xxx-4b",
  "id" : "a0865121f83b41cbafce65930a22a6e8",
  "local_name" : {
    "en_us" : "AZ2",
    "zh_cn" : "<Name_of_AZ2>"
  },
  "name" : "<Name_of_AZ2>",
  "port" : "8404",
  "specs" : {
    "BASIC" : true,
    "BASIC_IPV6" : true,
    "ENTERPRISE" : true,
    "ENTERPRISE_IPV6" : true,
    "PLATINUM" : true,
    "PLATINUM_IPV6" : false,
    "PROFESSIONAL" : true,
    "PROFESSIONAL_IPV6" : true,
    "TRIAL" : true,
    "PLATINUM_X2" : false,
    "PLATINUM_X3" : false,
    "PLATINUM_X4" : false,
    "PLATINUM_X5" : false,
    "PLATINUM_X6" : false,
    "PLATINUM_X7" : false,
    "PLATINUM_X8" : false
  }
}
}]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
```

```
"error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23.14 Querying Dedicated Gateways

Function

This API is used to query dedicated gateways.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances

Table 4-1356 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Table 4-1357 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
instance_id	No	String	Gateway ID.
instance_name	No	String	Gateway name.

Parameter	Mandatory	Type	Description
status	No	String	Gateway status. • Creating • CreateSuccess • CreateFail • Initing • Registering • Running • InitingFailed • RegisterFailed • Installing • InstallFailed • Updating • UpdateFailed • Rollbacking • RollbackSuccess • RollbackFailed • Deleting • DeleteFailed • Unregistering • UnRegisterFailed • CreateTimeout • InitTimeout • RegisterTimeout • InstallTimeout • UpdateTimeout • RollbackTimeout • DeleteTimeout • UnregisterTimeout • Starting • Freezing • Frozen • Restarting • RestartFail • Unhealthy • RestartTimeout

Request Parameters

Table 4-1358 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-1359** Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
instances	Array of RespInstanceBase objects	Gateway list.

Table 4-1360 RespInstanceBase

Parameter	Type	Description
id	String	Gateway ID.
project_id	String	ID of the tenant to which the gateway belongs.
instance_name	String	Gateway name.

Parameter	Type	Description
status	String	Instance status: • Creating: The instance is being created. • CreateSuccess: The instance is created successfully. • CreateFail: The instance fails to be created. • Initing: The instance is being initialized. • Registering: The instance is being registered. • Running: The instance is running. • InitingFailed: The instance fails to be initialized. • RegisterFailed: The instance fails to be registered. • Installing: The instance is being installed. • InstallFailed: The instance fails to be installed. • Updating: The instance is being upgraded. • UpdateFailed: The instance fails to be upgraded. • Rollbacking: The instance is being rolled back. • RollbackSuccess: The instance is rolled back successfully. • RollbackFailed: The instance fails to be rolled back. • Deleting: The instance is being deleted. • DeleteFailed: The instance fails to be deleted. • Unregistering: The instance is being deregistered. • UnRegisterFailed: The instance fails to be deregistered. • CreateTimeout: Creation of the instance times out. • InitTimeout: Initialization of the instance times out. • RegisterTimeout: Registration of the instance times out.

Parameter	Type	Description
		• InstallTimeout: Installation of the instance times out. • UpdateTimeout: Upgrading of the instance times out. • RollbackTimeout: Rollback of the instance times out. • DeleteTimeout: Deletion of the instance times out. • UnregisterTimeout: Deregistration of the instance times out. • Starting: The instance is being started. • Freezing: The instance is being frozen. • Frozen: The instance is frozen. • Restarting: The instance is being restarted. • RestartFail: The instance fails to be restarted. • Unhealthy: The instance is abnormal. • RestartTimeout: Restart of the instance times out. • Resizing: The instance specification is changing. • ResizeFailed: The instance specification fails to be changed. • ResizeTimeout: The instance specification change times out.

Parameter	Type	Description
instance_status	Integer	Instance status ID: • 1: Creating • 2: Created successfully • 3: Creation failed • 4: Initializing • 5: Registering • 6: Running • 7: Initialization failed • 8: Registration failed • 10: Installing • 11: Installation failed • 12: Upgrading • 13: Upgrade failed • 20: Rolling back • 21: Rolled back • 22: Rollback failed • 23: Deleting • 24: Deletion failed • 25: Deregistering • 26: Deregistration failed • 27: Creation timed out • 28: Initialization timed out • 29: Registration timed out • 30: Installation timed out • 31: Upgrade timed out • 32: Rollback timed out • 33: Deletion timed out • 34: Deregistration timed out • 35: Starting • 36: Freezing • 37: Frozen • 38: Restarting • 39: Restart failed • 40: Abnormal • 41: Restart timed out • 42: Changing specification • 43: Specification change failed • 44: Specification change timed out

Parameter	Type	Description
type	String	Gateway type. The default value is apig.
spec	String	Gateway edition. • BASIC • PROFESSIONAL • ENTERPRISE • PLATINUM • BASIC_IPV6 • PROFESSIONAL_IPV6 • ENTERPRISE_IPV6 • PLATINUM_IPV6
create_time	Long	Time when the gateway is created. The time is in the Unix timestamp format.
enterprise_project_id	String	Enterprise project ID. This parameter is required for an enterprise account.
eip_address	String	EIP bound to the gateway.
charging_mode	Integer	Billing mode of the gateway. • 0: pay-per-use • 1: This parameter is not used currently.
cbc_metadata	String	This parameter is not used currently.
loadbalancer_provider	String	Type of the load balancer used by the gateway. • LVS • ELB (available only in certain regions) Default: lvs
cbc_operation_locks	Array of CbcOperationLock objects	Cloud operations restriction lock

Table 4-1361 CbcOperationLock

Parameter	Type	Description
lock_scene	String	Restriction scenarios: • TO_PERIOD_LOCK: This parameter is not supported currently. • SPEC_CHG_LOCK: This parameter is not supported currently.
lock_source_id	String	ID of the object that initiates the restriction

Status code: 401**Table 4-1362** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1363** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1364** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 2,
  "size" : 2,
  "instances" : [ {
    "cbc_metadata" : "CS2006301043A28NF:00301-734023-0--0",
    "charging_mode" : 1,
    "create_time" : 1585302825070,
    "eip_address" : "xxx.xxx.xxx.xxx",
    "enterprise_project_id" : "0",
    "id" : "eddc4d25480b4cd6b512f270a1b8b341",
    "instance_name" : "apig-Enterprise_Project_Pay-per-Use",
    "instance_status" : 6,
    "project_id" : "73d69ae0cfcf460190522d06b60f05ad",
    "spec" : "PROFESSIONAL",
    "status" : "Running",
    "type" : "apig"
  }, {
    "charging_mode" : 0,
    "create_time" : 1594370987422,
    "eip_address" : "xxx.xxx.xxx.xxx",
    "enterprise_project_id" : "0",
    "id" : "2e2d613c64094a4a94ad38e7ca30adee",
    "instance_name" : "apig-autotest-apitest-nodelete",
    "instance_status" : 6,
    "project_id" : "73d69ae0cfcf460190522d06b60f05ad",
    "spec" : "PROFESSIONAL",
    "status" : "Running",
    "type" : "apig",
    "cbc_operation_locks" : [ {
      "lock_scene" : "TO_PERIOD_LOCK",
      "lock_source_id" : "CxxxxxxxxxxM"
    } ]
  } ]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23.15 Deleting a Dedicated Gateway

Function

This API is used to delete a dedicated gateway.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}

Table 4-1365 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1366 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 401**Table 4-1367** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1368** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1369** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1370** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 401**

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7302",
  "error_msg" : "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
204	No Content

Status Code	Description
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23.16 Modifying the Specifications of a Pay-Per-Use Gateway

Function

This API is used to create a specification change order of a pay-per-use gateway.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/postpaid-resize

Table 4-1371 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1372 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1373 Request body parameters

Parameter	Mandatory	Type	Description
spec_id	No	String	Target gateway specifications.

Response Parameters

Status code: 202

Table 4-1374 Response body parameters

Parameter	Type	Description
instance_id	String	Gateway ID.
message	String	Gateway scale-out information.
job_id	String	Task ID.

Status code: 401

Table 4-1375 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1376 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1377** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

```
{
  "spec_id" : "PROFESSIONAL"
}
```

Example Responses

Status code: 202

ACCEPTED

```
{
  "instance_id" : "6a7d71827fd54572b1f31aa9548fcc81",
  "message" : "JOB_ASSIGNED_FOR_RESIZE_0086l:The job JOB-5acb75c7565e42c997954774456eac79 is assigned to resize instance.",
  "job_id" : "JOB-5acb75c7565e42c997954774456eac79"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
202	ACCEPTED
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.23.17 Querying Gateway Constraints

Function

This API is used to query the constraints of a gateway.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/restriction

Table 4-1378 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1379 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1380 Response body parameters

Parameter	Type	Description
restrict_cidrs	Array of strings	CIDR block list of the restricted IP network segment.
resource_subnet_cidr	String	CIDR block of the IP network segment of the resource tenant.

Status code: 401

Table 4-1381 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1382 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1383 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1384 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "restrict_cidrs" : [ "127.0.0.1/32", "192.168.0.1/24" ],
  "resource_subnet_cidr" : "192.168.0.1/24"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7302",
  "error_msg" : "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.24 VPC Endpoint Management

4.24.1 Querying VPC Endpoint Connections

Function

This API is used to query the VPC endpoint connections of a gateway.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/vpc-endpoint/connections

Table 4-1385 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1386 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
id	No	String	Unique VPC endpoint ID.
marker_id	No	Integer	Packet ID of a VPC endpoint.
status	No	String	Connection status of a VPC endpoint. Options: • pendingAcceptance • accepted • rejected • failed

Request Parameters

Table 4-1387 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1388 Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1389 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
connections	Array of EndpointConnection objects	Connections.

Table 4-1390 EndpointConnection

Parameter	Type	Description
id	String	Connection ID.
marker_id	Integer	Connection packet ID.
created_at	String	Connection creation time. UTC time in the format YYYY-MM-DDTHH:MM:SSZ.
updated_at	String	Connection update time. UTC time in the format YYYY-MM-DDTHH:MM:SSZ.

Parameter	Type	Description
domain_id	String	Domain ID.
status	String	Connection status. • pendingAcceptance • creating • accepted • rejected • failed • deleting

Status code: 401**Table 4-1391** Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1392 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1393** Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1394 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1395** Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1396 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1397** Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1398 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 2,
  "size" : 1,
  "connections" : [ {
    "id" : "76ad893c-6a1e-4055-8019-fe9c9bd3204d",
    "marker_id" : 167960098,
    "created_at" : "2021-04-29T02:12:44Z",
    "updated_at" : "2021-04-29T02:12:45Z",
```

```
"domain_id" : "b70fde8e849b4e76a61dd8aa0ec05c81",  
"status" : "accepted"  
}]  
}
```

Status code: 401

Unauthorized

```
{  
  "error_code" : "APIC.7102",  
  "error_msg" : "Incorrect token or token resolution failed"  
}
```

Status code: 403

Forbidden

```
{  
  "error_code" : "APIC.7106",  
  "error_msg" : "No permissions to request for the method"  
}
```

Status code: 404

Resource Not Found

```
{  
  "error_code" : "APIC.7314",  
  "error_msg" : "Endpoint service not found"  
}
```

Status code: 500

Internal Server Error

```
{  
  "error_code" : "APIC.9007",  
  "error_msg" : "Failed to execute VCPEP request"  
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Resource Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.24.2 Accepting or Rejecting a VPC Endpoint Connection

Function

This API is used to accept or reject a VPC endpoint connection for a gateway.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/vpc-endpoint/connections/
action

Table 4-1399 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1400 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1401 Request body parameters

Parameter	Mandatory	Type	Description
action	Yes	String	Allow or reject connections. • receive • reject

Parameter	Mandatory	Type	Description
endpoints	Yes	Array of strings	VPC endpoints. Array Length: 1 - 50

Response Parameters

Status code: 200

Table 4-1402 Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1403 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
connections	Array of EndpointConnection objects	Connections.

Table 4-1404 EndpointConnection

Parameter	Type	Description
id	String	Connection ID.
marker_id	Integer	Connection packet ID.
created_at	String	Connection creation time. UTC time in the format YYYY-MM-DDTHH:MM:SSZ.
updated_at	String	Connection update time. UTC time in the format YYYY-MM-DDTHH:MM:SSZ.
domain_id	String	Domain ID.

Parameter	Type	Description
status	String	Connection status. • pendingAcceptance • creating • accepted • rejected • failed • deleting

Status code: 401**Table 4-1405** Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1406 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1407** Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1408 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1409 Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1410 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1411** Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1412 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

- Accept a connection from a VPC endpoint.

```
{
  "action": "receive",
  "endpoints": [ "9fa04c5e-64ec-4106-a014-2ad71ad9997d" ]
}
```

- Disable a VPC endpoint connection.

```
{
  "action": "reject",
  "endpoints": [ "9fa04c5e-64ec-4106-a014-2ad71ad9997d" ]
}
```

Example Responses

Status code: 200

OK

```
{
  "connections": [ {
```

```
{
  "id" : "9cf102d8-aaa0-44cf-8222-fd6f2c073887",
  "marker_id" : 167792784,
  "created_at" : "2021-05-07T14:20:14Z",
  "updated_at" : "2021-05-07T14:30:25Z",
  "domain_id" : "c90f12a0f1ee43bc90a1f4d17bce35bc",
  "status" : "accepted"
}]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Resource Not Found

```
{
  "error_code" : "APIC.7314",
  "error_msg" : "Endpoint service not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9007",
  "error_msg" : "Failed to execute VCPEP request"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Resource Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.24.3 Querying Whitelist Records of a VPC Endpoint Service

Function

This API is used to query the whitelist records of a gateway's VPC endpoint service.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions

Table 4-1413 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1414 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20

Parameter	Mandatory	Type	Description
permission	No	String	Permission account ID in format "iam:domain::domain_id". Fuzzy search is supported.

Request Parameters

Table 4-1415 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1416 Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1417 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
permissions	Array of EndpointPermission objects	Whitelist records.

Table 4-1418 EndpointPermission

Parameter	Type	Description
id	String	Record ID.
permission	String	Permission rules.
created_at	String	Creation time.

Status code: 401**Table 4-1419** Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1420 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1421** Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1422 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1423 Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1424 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1425 Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1426 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 2,
  "size" : 1,
  "permissions" : [ {
    "id" : "e4a7ba21-1e5c-43cc-977d-4aeeacb937ec",
    "permission" : "iam:domain::821a2d452de64bcd52319967f8a06b9",
    "created_at" : "2021-05-07T14:10:49Z"
  } ]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Resource Not Found

```
{
  "error_code" : "APIC.7314",
  "error_msg" : "Endpoint service not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9007",
  "error_msg" : "Failed to execute VCPEP request"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Resource Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.24.4 Adding Whitelist Records for a VPC Endpoint Service

Function

This API is used to add whitelist records in batches for a gateway's VPC endpoint service.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions/
batch-add

Table 4-1427 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1428 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1429 Request body parameters

Parameter	Mandatory	Type	Description
permissions	Yes	Array of strings	Whitelist records. Each whitelist record is in the format of "iam:domain::Authorized_account_ID". The account ID contains 32 characters, including only letters (a–f) and digits. An asterisk (*) means that all users have access. Array Length: 1 - 50

Response Parameters

Status code: 200

Table 4-1430 Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1431 Response body parameters

Parameter	Type	Description
permissions	Array of strings	Whitelist records. Each whitelist record is in the format of "iam:domain::Authorized_account_ID". The account ID contains 32 characters, including only letters (a-f) and digits. An asterisk (*) means that all users have access. Array Length: 1 - 50

Status code: 401

Table 4-1432 Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1433 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1434 Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1435 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1436** Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1437 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1438** Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1439 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Add whitelist records for a vpc endpoint service.

```
{  
  "permissions" : [ "iam:domain::7cc2018e40394f7c9692f1713e76234d" ]  
}
```

Example Responses

Status code: 200

OK

```
{  
  "permissions" : [ "iam:domain::930ba6b0ea64457e8ed1861e596c7a9a" ]  
}
```

Status code: 401

Unauthorized

```
{  
  "error_code" : "APIC.7102",  
  "error_msg" : "Incorrect token or token resolution failed"  
}
```

Status code: 403

Forbidden

```
{  
  "error_code" : "APIC.7106",  
  "error_msg" : "No permissions to request for the method"  
}
```

Status code: 404

Resource Not Found

```
{  
  "error_code" : "APIC.7314",  
  "error_msg" : "Endpoint service not found"  
}
```

Status code: 500

Internal Server Error

```
{  
  "error_code" : "APIC.9007",  
  "error_msg" : "Failed to execute VCPEP request"  
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Resource Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.24.5 Deleting Whitelist Records of a VPC Endpoint Service

Function

This API is used to delete whitelist records of a gateway's VPC endpoint service in batches.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions/
batch-delete

Table 4-1440 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1441 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1442 Request body parameters

Parameter	Mandatory	Type	Description
permissions	Yes	Array of strings	Whitelist records. Each whitelist record is in the format of "iam:domain::Authorized_account_ID". The account ID contains 32 characters, including only letters (a–f) and digits. An asterisk (*) means that all users have access. Array Length: 1 - 50

Response Parameters

Status code: 200

Table 4-1443 Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1444 Response body parameters

Parameter	Type	Description
permissions	Array of strings	Whitelist records. Each whitelist record is in the format of "iam:domain::Authorized_account_ID". The account ID contains 32 characters, including only letters (a–f) and digits. An asterisk (*) means that all users have access. Array Length: 1 - 50

Status code: 401

Table 4-1445 Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1446 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1447** Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1448 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1449** Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1450 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1451 Response header parameters

Parameter	Type	Description
x-request-id	String	Request ID.

Table 4-1452 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Delete whitelist records for a vpc endpoint service.

```
{
  "permissions" : [ "iam:domain::7cc2018e40394f7c9692f1713e76234d" ]
}
```

Example Responses

Status code: 200

OK

```
{
  "permissions" : [ "iam:domain::930ba6b0ea64457e8ed1861e596c7a9a" ]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Resource Not Found

```
{
  "error_code" : "APIC.7314",
  "error_msg" : "Endpoint service not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9007",
  "error_msg" : "Failed to execute VCPEP request"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Resource Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.25 Gateway Tag Management

4.25.1 Querying All Gateway Tags of a Project

Function

This API is used to query all gateway tags of a project.

Constraints

Only users who have been authorized with a policy containing action `apig:instanceTags:list` can call this API.

Calling Method

For details, see [Calling APIs](#).

URI

GET `/v2/{project_id}/apigw/instance-tags`

Table 4-1453 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Request Parameters

Table 4-1454 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1455 Response body parameters

Parameter	Type	Description
tags	Array of TmsKeyValues objects	Tags bound to all gateways in the project.

Table 4-1456 TmsKeyValues

Parameter	Type	Description
key	String	Key. Include UTF-8 letters, digits, spaces, or special characters (<code>_</code> , <code>.</code> , <code>+</code> , <code>-</code> , <code>@</code>). Do not start with <code>_sys_</code> because it is a system label. Minimum: 1 Maximum: 128

Parameter	Type	Description
values	Array of strings	Value. You can enter letters, digits, and spaces or other special characters (._:/=+-@) in UTF-8 format.

Status code: 401**Table 4-1457** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1458** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1459** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "tags" : [ {
    "key" : "test-key",
    "values" : [ "test-value1", "test-value2" ]
  } ]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.25.2 Querying Tags of a Gateway

Function

This API is used to query all tags of a gateway.

Constraints

Only users who have been authorized with a policy containing actions `apig:instanceTags:list` and `apig:instances:get` can call this API.

Calling Method

For details, see [Calling APIs](#).

URI

GET `/v2/{project_id}/apigw/instances/{instance_id}/instance-tags`

Table 4-1460 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1461 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1462 Response body parameters

Parameter	Type	Description
tags	Array of TmsKeyValue objects	Tags bound to the gateway.

Table 4-1463 TmsKeyValue

Parameter	Type	Description
key	String	Key. Include UTF-8 letters, digits, spaces, or special characters (_.:/+@). Do not start with _sys_ because it is a system label. Minimum: 1 Maximum: 128
value	String	Value. You can enter letters, digits, and spaces or other special characters (_.:/+@) in UTF-8 format. Minimum: 0 Maximum: 255

Status code: 401**Table 4-1464** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1465** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1466** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "tags" : [ {
    "key" : "test-key",
    "value" : "test-vau"
  } ]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.25.3 Adding or Deleting Tags of a Gateway

Function

This API is used to add tags to a gateway or delete the tags of a gateway.

Constraints

Only users who have been authorized with a policy containing actions `apig:instances:get`, `apig:instanceTags:create`, and `apig:instanceTags:delete` can call this API.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/instance-tags/action

Table 4-1467 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1468 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1469 Request body parameters

Parameter	Mandatory	Type	Description
action	Yes	String	Operation: create and delete.
tags	Yes	Array of TmsKeyValue objects	Tags. A maximum of 20 tags can be created for a gateway. Array Length: 0 - 20

Table 4-1470 TmsKeyValue

Parameter	Mandatory	Type	Description
key	No	String	Key. Include UTF-8 letters, digits, spaces, or special characters (._:=-@). Do not start with _sys_ because it is a system label. Minimum: 1 Maximum: 128
value	No	String	Value. You can enter letters, digits, and spaces or other special characters (._:=-@) in UTF-8 format. Minimum: 0 Maximum: 255

Response Parameters

Status code: 204

No Content

Status code: 401

Table 4-1471 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1472 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1473** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

- Adding tags for a gateway

```
{
  "action": "create",
  "tags": [ {
    "key": "test-key",
    "value": "test-value"
  } ]
}
```

- Deleting tags of a gateway

```
{
  "action": "delete",
  "tags": [ {
    "key": "test-key1",
    "value": "test-value"
  }, {
    "key": "test-key2"
  } ]
}
```

Example Responses

Status code: 401

Unauthorized

```
{
  "error_code": "APIC.7102",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIC.7106",
  "error_msg": "No permissions to request for the method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000"
}
```

Status Codes

Status Code	Description
204	No Content
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.25.4 Querying the Number of Gateways with a Specified Tag

Function

This API is used to query the number of gateways with a specified tag.

Constraints

When a policy is used to authorize users, this API can be called only when the apig:instance:getNumByTags action is contained.

Calling MethodFor details, see [Calling APIs](#).**URI**

POST /v2/{project_id}/apigw/resource-instances/count

Table 4-1474 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Request Parameters

Table 4-1475 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1476 Request body parameters

Parameter	Mandatory	Type	Description
without_any_tag	No	Boolean	Resources to be queried contain no tags. If this parameter is set to true , all resources without tags are queried. In this case, the tags field is ignored. If this parameter is set to false or not specified, it does not take effect.
tags	No	Array of TmsKeyValues objects	Included tags. A maximum of 20 keys are included. Each key can have a maximum of 20 values. If no tag filtering criteria is specified, full data is returned. Array Length: 0 - 20
sys_tags	No	Array of TmsKeyValues objects	Enterprise project. Only the op_service permission can use this field to filter resources. If sys_tags is not used, resources are filtered by tag . If no tag filtering criteria is specified, full data is returned. Array Length: 0 - 1

Parameter	Mandatory	Type	Description
matches	No	Array of TmsMatches KeyValue objects	Search criteria. The tag key is the field to match. Currently, only resource_name is supported. The tag value indicates the matched value. Check whether fuzzy match is required based on the key value. For example, if key is set to resource_name , prefix search is performed.

Table 4-1477 TmsKeyValues

Parameter	Mandatory	Type	Description
key	No	String	Key. Include UTF-8 letters, digits, spaces, or special characters (<code>_./:=+-@</code>). Do not start with <code>_sys_</code> because it is a system label. Minimum: 1 Maximum: 128
values	No	Array of strings	Value. You can enter letters, digits, and spaces or other special characters (<code>_./:=+-@</code>) in UTF-8 format.

Table 4-1478 TmsMatchesKeyValue

Parameter	Mandatory	Type	Description
key	No	String	Specifies the field to be matched. • <code>resource_name</code> indicates that the APIG instance name is used for matching.

Parameter	Mandatory	Type	Description
value	No	String	Indicates the value. The value can contain UTF-8 letters, digits, spaces, and the following characters: (_ : / = + - @) : / = + - @ Maximum: 255

Response Parameters

Status code: 200

Table 4-1479 Response body parameters

Parameter	Type	Description
total_count	Integer	Total number of records.

Status code: 401

Table 4-1480 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1481 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1482 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

- Querying the number of gateways with a specified tag

```
{
  "without_any_tag" : false,
  "tags" : [ {
    "key" : "test-key",
    "values" : [ "test-value" ]
  } ],
  "matches" : [ {
    "key" : "resource_name",
    "value" : "test-apig"
  } ]
}
```
- Querying the number of gateways with a specified enterprise project ID

```
{
  "without_any_tag" : false,
  "sys_tags" : [ {
    "key" : "_sys_enterprise_project_id",
    "values" : [ "0" ]
  } ],
  "matches" : [ {
    "key" : "resource_name",
    "value" : "test-apig"
  } ]
}
```

Example Responses

Status code: 200

OK

```
{
  "total_count" : 20
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 500

Internal Server Error

```
{  
  "error_code" : "APIC.9000"  
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.25.5 Querying Gateways by Tag

Function

This API is used to query gateways by tag.

Constraints

When a policy is used to authorize users, this API can be called only when the apig:instance:listByTags action is contained.

Calling MethodFor details, see [Calling APIs](#).**URI**

POST /v2/{project_id}/apigw/resource-instances/filter

Table 4-1483 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Table 4-1484 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20

Request Parameters

Table 4-1485 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1486 Request body parameters

Parameter	Mandatory	Type	Description
without_any_tag	No	Boolean	Resources to be queried contain no tags. If this parameter is set to true , all resources without tags are queried. In this case, the tags field is ignored. If this parameter is set to false or not specified, it does not take effect.

Parameter	Mandatory	Type	Description
tags	No	Array of TmsKeyValues objects	Included tags. A maximum of 20 keys are included. Each key can have a maximum of 20 values. If no tag filtering criteria is specified, full data is returned. Array Length: 0 - 20
sys_tags	No	Array of TmsKeyValues objects	Enterprise project. Only the op_service permission can use this field to filter resources. If sys_tags is not used, resources are filtered by tag . If no tag filtering criteria is specified, full data is returned. Array Length: 0 - 1
matches	No	Array of TmsMatchesKeyValues objects	Search criteria. The tag key is the field to match. Currently, only resource_name is supported. The tag value indicates the matched value. Check whether fuzzy match is required based on the key value. For example, if key is set to resource_name , prefix search is performed.

Table 4-1487 TmsKeyValues

Parameter	Mandatory	Type	Description
key	No	String	Key. Include UTF-8 letters, digits, spaces, or special characters (<code>_./:=+-@</code>). Do not start with <code>_sys_</code> because it is a system label. Minimum: 1 Maximum: 128
values	No	Array of strings	Value. You can enter letters, digits, and spaces or other special characters (<code>_./:=+-@</code>) in UTF-8 format.

Table 4-1488 TmsMatchesKeyValue

Parameter	Mandatory	Type	Description
key	No	String	Specifies the field to be matched. resource_name indicates that the APIG instance name is used for matching.
value	No	String	Indicates the value. The value can contain UTF-8 letters, digits, spaces, and the following characters: (_ . : / = + - @) Maximum: 255

Response Parameters

Status code: 200

Table 4-1489 Response body parameters

Parameter	Type	Description
resources	Array of TmsResourceResp objects	Gateways
total_count	Integer	Total number of records.

Table 4-1490 TmsResourceResp

Parameter	Type	Description
resource_id	String	Gateway ID.
resource_detail	String	Detailed description of the gateway. Not supported.
resource_name	String	Gateway name.
tags	Array of TmsKeyValue objects	Tags bound to the gateway. Array Length: 0 - 20

Table 4-1491 TmsKeyValue

Parameter	Type	Description
key	String	Key. Include UTF-8 letters, digits, spaces, or special characters (_.:/+@). Do not start with _sys_ because it is a system label. Minimum: 1 Maximum: 128
value	String	Value. You can enter letters, digits, and spaces or other special characters (_.:/+@) in UTF-8 format. Minimum: 0 Maximum: 255

Status code: 401**Table 4-1492** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1493** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1494** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Example Requests

- Filtering gateways by tag

```
{
  "without_any_tag" : false,
  "tags" : [ {
    "key" : "test-key",
    "values" : [ "test-value" ]
  } ],
  "matches" : [ {
    "key" : "resource_name",
    "value" : "test-apig"
  } ]
}
```

- Filtering gateways by enterprise project IDs

```
{
  "without_any_tag" : false,
  "sys_tags" : [ {
    "key" : "_sys_enterprise_project_id",
    "values" : [ "0" ]
  } ],
  "matches" : [ {
    "key" : "resource_name",
    "value" : "test-apig"
  } ]
}
```

Example Responses

Status code: 200

Returned gateways

```
{
  "resources" : [ {
    "resource_id" : "e120108ac331422cb539d8609e9a7bb2",
    "resource_detail" : null,
    "resource_name" : "apig_instance",
    "tags" : [ {
      "key" : "test-key",
      "value" : "test-value"
    } ]
  } ],
  "total_count" : 1
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000"
}
```

Status Codes

Status Code	Description
200	Returned gateways
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.26 Microservice Center Management

4.26.1 Importing a Microservice

Function

This API is used to import a microservice.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/microservice/import

Table 4-1495 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1496 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1497 Request body parameters

Parameter	Mandatory	Type	Description
group_info	Yes	Microservice Group object	Information about the API group to import a microservice to.
service_type	Yes	String	Microservice center type. Options: • CSE: CSE microservice registration center. • CCE: CCE workload • CCE_SERVICE: CCE Service (not supported currently) • NACOS: Nacos registration center. nacos_info is mandatory.

Parameter	Mandatory	Type	Description
protocol	No	String	Request protocol used by APIG to access the microservice. • HTTP • HTTPS Default: HTTPS
apis	Yes	Array of Microservice ApiCreate objects	Imported APIs. Array Length: 1 - 50
backend_timeout	No	Integer	Timeout allowed for APIG to request the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000, and the default value is 5000. Unit: ms. Minimum: 1 Default: 5000
auth_type	No	String	API authentication mode. By default, authentication is not required. • NONE • APP • IAM Default: NONE
cors	No	Boolean	Whether CORS is supported. By default, it is not supported. • true: Supported. • false: Not supported. Default: false
cse_info	No	MicroserviceInfoCSECreate object	CSE microservice details. This parameter is required if service_type is set to CSE.
cce_info	No	MicroserviceInfoCCECreate object	CCE workload details. This parameter is required if service_type is set to CCE.

Parameter	Mandatory	Type	Description
cce_service_info	No	MicroServiceInfoCCEServiceCreate object	CCE Service details. This parameter is required if service_type is set to CCE_SERVICE.
nacos_info	No	MicroServiceInfoNacosBase object	Nacos basic information.

Table 4-1498 MicroserviceGroup

Parameter	Mandatory	Type	Description
group_id	No	String	An existing group. If this parameter is left empty, a new group is created. Minimum: 0 Maximum: 64
group_name	No	String	Name of the API group. This parameter is required when group_id is empty. Enter 3 to 255 characters, starting with a letter or digit. Only letters, digits, and these special characters are allowed: -_./:() Minimum: 3 Maximum: 255
app_id	No	String	Integration application to which the new group belongs. This parameter is required when group_id is empty. Minimum: 0 Maximum: 64

Table 4-1499 MicroserviceApiCreate

Parameter	Mandatory	Type	Description
name	No	String	API name. Start with a letter or digit, and use only letters, digits, and these special characters: -_./:() Minimum: 3 Maximum: 255
req_method	No	String	Request method. Default: ANY
req_uri	Yes	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. /apic/health_check is the preset health check path of APIG. If req_method=GET is passed, req_uri=/apic/health_check is not supported. NOTE The address must comply with the URI specifications. Minimum: 1 Maximum: 512
match_mode	No	String	API matching mode. • SWA: Prefix match. • NORMAL: Exact match. Default value: NORMAL Default: SWA

Table 4-1500 MicroServiceInfoCSECreate

Parameter	Mandatory	Type	Description
engine_id	Yes	String	Microservice engine ID. Maximum: 64

Parameter	Mandatory	Type	Description
service_id	Yes	String	Microservice ID. Maximum: 64
version	Yes	String	Microservice version. Maximum: 64

Table 4-1501 MicroServiceInfoCCECreate

Parameter	Mandatory	Type	Description
cluster_id	Yes	String	CCE cluster ID. Maximum: 64
namespace	Yes	String	Namespace. Maximum: 64
workload_type	Yes	String	Workload type. • deployment • statefulset • daemonset
app_name	No	String	App name. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
label_key	No	String	Service label key. Start with a letter or digit, and use only letters, digits, and these special characters: -_./:(). (1 to 64 characters) Minimum: 1 Maximum: 64
label_value	No	String	Service label value. Start with a letter, and include only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
version	No	String	Workload version. Maximum: 64

Parameter	Mandatory	Type	Description
port	Yes	Integer	Listening port No. of the workload. Minimum: 1 Maximum: 65535
labels	No	Array of MicroserviceLabel objects	Workload label list.

Table 4-1502 MicroserviceLabel

Parameter	Mandatory	Type	Description
label_name	Yes	String	Tag name. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63
label_value	Yes	String	Tag value. Start and end with a letter or digit. Use only letters, digits, hyphens (-), underscores (_), and periods (.). (Max. 63 characters.) Minimum: 1 Maximum: 63

Table 4-1503 MicroServiceInfoCCEServiceCreate

Parameter	Mandatory	Type	Description
cluster_id	Yes	String	CCE cluster ID. Maximum: 64
namespace	Yes	String	Namespace. 1 to 63 characters. Use lowercase letters, digits, and hyphens (-). Start with a letter and end with a letter or digit. Minimum: 1 Maximum: 63

Parameter	Mandatory	Type	Description
service_name	Yes	String	Service name. Start with a letter, and use only letters, digits, periods (.), hyphens (-), and underscores (_). (1 to 64 characters) Minimum: 1 Maximum: 64
port	No	Integer	Service listening port. For a multi-port service, you only need to enter one port number. Minimum: 1 Maximum: 65535

Table 4-1504 MicroServiceInfoNacosBase

Parameter	Mandatory	Type	Description
namespace	No	String	Namespace ID. If the default namespace public is used, leave this parameter empty. Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
cluster_name	No	String	Cluster name. The default value is DEFAULT . Only letters, numbers, hyphens (-), underscores (_) are allowed. Max.: 64 characters Minimum: 0 Maximum: 64
group_name	No	String	Group name. The default value is DEFAULT_GROUP . Only letters, numbers, hyphens (-), underscores (_), periods (.), and colons (:) are allowed. Max.: 128 characters Minimum: 0 Maximum: 128

Parameter	Mandatory	Type	Description
service_name	Yes	String	Microservice name. The value cannot start with @ or contain @@. Max.: 512 characters Minimum: 1 Maximum: 512
server_config	Yes	Array of NacosServerConfig objects	Nacos server configurations. Array Length: 1 - 9
user_info	Yes	NacosUserInfo object	Nacos user information.

Table 4-1505 NacosServerConfig

Parameter	Mandatory	Type	Description
ip_address	Yes	String	IP address of the Nacos server. Minimum: 7 Maximum: 128
port	Yes	Integer	Port number of the Nacos server. Range: 1–65535. Minimum: 1 Maximum: 65535
grpc_port	No	Integer	gRPC port number of the Nacos server. Default: port number + 1000 Range: 1–65535. Minimum: 1 Maximum: 65535

Table 4-1506 NacosUserInfo

Parameter	Mandatory	Type	Description
user_name	Yes	String	Nacos username. Minimum: 1 Maximum: 64
password	Yes	String	Nacos password. Minimum: 1 Maximum: 64

Response Parameters

Status code: 201

Table 4-1507 Response body parameters

Parameter	Type	Description
vpc_channel_id	String	VPC channel ID.
api_group_id	String	API group ID.
apis	Array of MicroserviceImportApiResp objects	Imported APIs.

Table 4-1508 MicroserviceImportApiResp

Parameter	Type	Description
name	String	API name.
req_uri	String	Request path.
req_method	String	Request method.
id	String	API ID.
match_mode	String	API matching mode. - SWA: Prefix match. - NORMAL: Exact match. Default value: SWA

Status code: 400

Table 4-1509 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1510 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1511** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1512** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1513** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

- Importing a CSE microservice

```
{
  "group_info": {
    "group_id": "6329eaa17736412b988536179cd8d662",
    "group_name": "",
    "app_id": ""
  },
  "service_type": "CSE",
  "protocol": "HTTPS",
  "apis": [ {
```

```
"name" : "api1",
"req_method" : "ANY",
"req_uri" : "/test",
"match_mode" : "SWA"
}],
"backend_timeout" : 5000,
"auth_type" : "NONE",
"cors" : false,
"cse_info" : {
  "engine_id" : "fde2c21c-5bd9-40f0-ad6a-81e4b6782805a",
  "service_id" : "92919f98fba80c2df13cc285c983946c90e635ff",
  "version" : "1.0.0"
}
}
```

- Importing a CCE Deployment

```
{
  "group_info" : {
    "group_id" : "6329eaa17736412b988536179cd8d662",
    "group_name" : "",
    "app_id" : ""
  },
  "service_type" : "CCE",
  "protocol" : "HTTPS",
  "apis" : [ {
    "name" : "dp",
    "req_method" : "ANY",
    "req_uri" : "/test",
    "match_mode" : "SWA"
  } ],
  "backend_timeout" : 5000,
  "auth_type" : "NONE",
  "cors" : false,
  "cce_info" : {
    "cluster_id" : "11069278-f9f8-11ec-b1b2-0255ac100b06",
    "namespace" : "test",
    "workload_type" : "deployment",
    "app_name" : "dp",
    "port" : 80,
    "labels" : [ {
      "label_name" : "cluster_id",
      "label_value" : "c429700c-5dc4-482a-9c0e-99f6c0635113"
    } ]
  }
}
```

Example Responses

Status code: 201

success

- Example 1

```
{
  "vpc_channel_id" : "9d075537ff314a5e8e5c98bf29549b89",
  "api_group_id" : "6329eaa17736412b988536179cd8d662",
  "apis" : [ {
    "id" : "72e667087fe140529f81995b213dadbe",
    "name" : "api1",
    "req_uri" : "/test",
    "req_method" : "ANY",
    "match_mode" : "SWA"
  } ]
}
```

- Example 2

```
{
  "vpc_channel_id" : "3f56e9d4a747486caa4cfb59a47b6854",

```

```
"api_group_id" : "6329eaa17736412b988536179cd8d662",
"apis" : [ {
  "id" : "3b52e2c05710470b88e283deb0a805e6",
  "name" : "dp_b09d",
  "req_uri" : "/test",
  "req_method" : "ANY",
  "match_mode" : "SWA"
} ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:f0fa1789-3b76-433b-a787-9892951c620ec"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	success
400	Bad Request
401	Unauthorized

Status Code	Description
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.27 SSL Certificate Management

4.27.1 Querying SSL Certificates

Function

This API is used to query the SSL certificates.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/certificates

Table 4-1514 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Table 4-1515 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
name	No	String	Certificate name.
common_name	No	String	Certificate domain name.
signature_algorithm	No	String	Certificate signature algorithm.
type	No	String	Certificate scope.
instance_id	Yes	String	ID of the gateway to which the certificate belongs.
algorithm_type	No	String	Certificate algorithm type: • RSA • ECC • SM2

Request Parameters

Table 4-1516 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1517 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
certs	Array of CertBase objects	Certificate basic content.

Table 4-1518 CertBase

Parameter	Type	Description
id	String	Certificate ID.
name	String	Certificate name.
type	String	Certificate type. • global: Global certificate. • instance: Gateway certificate.
instance_id	String	Gateway ID. • If type is set to global, the default value is common. • If type is set to instance, a gateway ID is displayed.
project_id	String	Project ID.
common_name	String	Domain name.
san	Array of strings	SAN domain name.
not_after	String	Expiration time.
signature_algorithm	String	Signature algorithm.
create_time	String	Creation time.
update_time	String	Update time.
is_has_trusted_root_ca	Boolean	Whether a trusted root certificate (CA) exists. The value is true if trusted_root_ca exists in the bound certificate. Default: false

Parameter	Type	Description
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2

Status code: 400**Table 4-1519** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1520** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1521** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1522** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "certs" : [ {
    "id" : "a27be832f2e9441c8127fe48e3b5ac67",
    "name" : "cert_demo",
    "type" : "instance",
    "project_id" : "73d69ae0cfcf460190522d06b60f05ad",
    "instance_id" : "f0fa1789-3b76-433b-a787-9892951c620e",
    "common_name" : "apigtest.example.com",
    "san" : [ "apigtest.example.com", "*.san.com" ],
    "not_after" : "2021-04-26T09:03:30Z",
    "signature_algorithm" : "SHA256-RSA",
    "create_time" : "2021-08-26T07:27:06.304004Z",
    "update_time" : "2021-08-26T07:27:06.304004Z",
    "algorithm_type" : "RSA"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:dict_name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.27.2 Creating an SSL Certificate

Function

This API is used to create an SSL certificate.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/certificates

Table 4-1523 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Request Parameters

Table 4-1524 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1525 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Certificate name. It can contain 4 to 50 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
cert_content	Yes	String	Certificate content.
private_key	Yes	String	Certificate private key.
type	No	String	Certificate scope. Default: global
instance_id	No	String	Gateway ID. This parameter is required if type is set to instance.
trusted_root_ca	No	String	Trusted root certificate (CA).
algorithm_type	No	String	Certificate algorithm type: • RSA • ECC • SM2
cert_content_sign	No	String	Signature certificate content. This parameter is mandatory only when algorithm_type is set to SM2. Maximum: 8092
private_key_sign	No	String	Signature private key content. This parameter is mandatory only when algorithm_type is set to SM2. Maximum: 8092

Response Parameters

Status code: 200

Table 4-1526 Response body parameters

Parameter	Type	Description
id	String	Certificate ID.
name	String	Certificate name.
type	String	Certificate type. • global: Global certificate. • instance: Gateway certificate.
instance_id	String	Gateway ID. • If type is set to global, the default value is common. • If type is set to instance, a gateway ID is displayed.
project_id	String	Project ID.
common_name	String	Domain name.
san	Array of strings	SAN domain name.
not_after	String	Expiration time.
signature_algorithm	String	Signature algorithm.
create_time	String	Creation time.
update_time	String	Update time.
is_has_trusted_root_ca	Boolean	Whether a trusted root certificate (CA) exists. The value is true if trusted_root_ca exists in the bound certificate. Default: false
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2
version	Integer	Version.
organization	Array of strings	Company or organization.

Parameter	Type	Description
organizational_unit	Array of strings	Department.
locality	Array of strings	City.
state	Array of strings	State or province.
country	Array of strings	Country or region.
not_before	String	Effective time.
serial_number	String	Serial number.
issuer	Array of strings	Issuer.

Status code: 400**Table 4-1527** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1528** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1529** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1530 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1531** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Creating an SSL certificate

```
{
  "name" : "cert_demo",
  "private_key" : ""-----BEGIN PRIVATE KEY-----THIS IS YOUR PRIVATE KEY-----END PRIVATE KEY-----\\n",
  "cert_content" : ""-----BEGIN CERTIFICATE-----THIS IS YOUR CERT CONTENT-----END CERTIFICATE-----\\n",
  "type" : "instance",
  "instance_id" : "f0fa1789-3b76-433b-a787-9892951c620e"
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "a27be832f2e9441c8127fe48e3b5ac67",
  "name" : "cert_demo",
  "common_name" : "apigtest.example.com",
  "san" : [ "apigtest.example.com", "*.san.com" ],
  "version" : 3,
  "organization" : [ "XX" ],
  "organizational_unit" : [ "IT" ],
  "locality" : [ "XX" ],
  "state" : [ "XX" ],
  "country" : [ "XX" ],
  "not_before" : "2019-06-01T00:00:00Z",
  "not_after" : "2031-08-16T06:36:13Z",
  "serial_number" : "13010",
  "issuer" : [ "XXSSL Inc" ],
  "signature_algorithm" : "SHA256-RSA",
  "create_time" : "2021-08-20T02:03:53Z",
  "update_time" : "2021-08-20T02:03:53Z",
  "algorithm_type" : "RSA"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.3325",
  "error_msg" : "The API quota name already exists"
}
```

Status code: 401**Unauthorized**

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403**Forbidden**

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404**Not Found**

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:f0fa1789-3b76-433b-a787-9892951c620ec"
}
```

Status code: 500**Internal Server Error**

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.27.3 Binding a Domain Name with SSL Certificates

Function

This API is used to bind a domain name with SSL certificates. Currently, only one certificate ID can be specified in `certificate_ids`. For gateways with custom inbound ports, the same domain name is bound to a certificate at the same time. Enabling or disabling client verification takes effect for different ports of the same domain name.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificates/attach

Table 4-1532 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.
domain_id	Yes	String	Domain ID.

Request Parameters

Table 4-1533 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1534 Request body parameters

Parameter	Mandatory	Type	Description
certificate_ids	Yes	Array of strings	Certificate IDs.
verified_client_certificate_enabled	No	Boolean	Whether to enable client certificate verification. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist.

Response Parameters

Status code: 204

OK

Status code: 400

Table 4-1535 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1536 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1537 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1538** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1539** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Binding a domain name with SSL certificates

```
{
  "certificate_ids" : [ "a27be832f2e9441c8127fe48e3b5ac67" ]
}
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:domain_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3020",
  "error_msg" : "The URL domain does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.27.4 Unbinding a Domain Name's SSL Certificates

Function

This API is used to unbind a domain name's SSL certificates. Currently, only one certificate ID can be specified in `certificate_ids`. For gateways with custom inbound ports, the same domain name will be unbound from the certificate at the same time.

Calling MethodFor details, see [Calling APIs](#).**URI**

```
POST /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/
domains/{domain_id}/certificates/detach
```

Table 4-1540 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
group_id	Yes	String	API group ID.
domain_id	Yes	String	Domain ID.

Request Parameters

Table 4-1541 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1542 Request body parameters

Parameter	Mandatory	Type	Description
certificate_ids	Yes	Array of strings	Certificate IDs.
verified_client_certificate_enabled	No	Boolean	Whether to enable client certificate verification. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist.

Response Parameters

Status code: 204

OK

Status code: 400

Table 4-1543 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1544** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1545** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1546** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1547** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Unbinding a domain name's SSL certificates

```
{
  "certificate_ids" : [ "a27be832f2e9441c8127fe48e3b5ac67" ]
}
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:domain_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3020",
  "error_msg" : "The URL domain does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	OK
400	Bad Request

Status Code	Description
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.27.5 Querying Certificate Details

Function

This API is used to query the details about a certificate.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/certificates/{certificate_id}

Table 4-1548 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
certificate_id	Yes	String	Certificate ID.

Request Parameters

Table 4-1549 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-1550** Response body parameters

Parameter	Type	Description
id	String	Certificate ID.
name	String	Certificate name.
type	String	Certificate type. • global: Global certificate. • instance: Gateway certificate.
instance_id	String	Gateway ID. • If type is set to global, the default value is common. • If type is set to instance, a gateway ID is displayed.
project_id	String	Project ID.
common_name	String	Domain name.
san	Array of strings	SAN domain name.
not_after	String	Expiration time.
signature_algorithm	String	Signature algorithm.
create_time	String	Creation time.
update_time	String	Update time.

Parameter	Type	Description
is_has_trusted_root_ca	Boolean	Whether a trusted root certificate (CA) exists. The value is true if trusted_root_ca exists in the bound certificate. Default: false
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2
version	Integer	Version.
organization	Array of strings	Company or organization.
organizational_unit	Array of strings	Department.
locality	Array of strings	City.
state	Array of strings	State or province.
country	Array of strings	Country or region.
not_before	String	Effective time.
serial_number	String	Serial number.
issuer	Array of strings	Issuer.

Status code: 400**Table 4-1551** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1552** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1553** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1554** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1555** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "id" : "a27be832f2e9441c8127fe48e3b5ac67",
  "name" : "cert_demo",
  "common_name" : "apigtest.example.com",
  "san" : [ "apigtest.example.com", "*.san.com" ],
  "version" : 3,
  "organization" : [ "XX" ],
  "organizational_unit" : [ "IT" ],
  "locality" : [ "XX" ],
  "state" : [ "XX" ],
  "country" : [ "XX" ],
  "not_before" : "2019-06-01T00:00:00Z",
  "not_after" : "2031-08-16T06:36:13Z",
}
```

```
"serial_number" : "13010",  
"issuer" : [ "XXSSL Inc" ],  
"signature_algorithm" : "SHA256-RSA",  
"create_time" : "2021-08-20T02:03:53Z",  
"update_time" : "2021-08-20T02:03:53Z",  
"algorithm_type" : "RSA"  
}
```

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2012",  
  "error_msg" : "Invalid parameter value,parameterName:domain_id. Please refer to the support  
documentation"  
}
```

Status code: 401

Unauthorized

```
{  
  "error_code" : "APIG.1002",  
  "error_msg" : "Incorrect token or token resolution failed"  
}
```

Status code: 403

Forbidden

```
{  
  "error_code" : "APIG.1005",  
  "error_msg" : "No permissions to request this method"  
}
```

Status code: 404

Not Found

```
{  
  "error_code" : "APIG.3020",  
  "error_msg" : "The URL domain does not exist"  
}
```

Status code: 500

Internal Server Error

```
{  
  "error_code" : "APIG.9999",  
  "error_msg" : "System error"  
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.27.6 Deleting an SSL Certificate

Function

This API is used to delete an SSL certificate. Only certificates that are not bound to any domain name can be deleted.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/certificates/{certificate_id}

Table 4-1556 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
certificate_id	Yes	String	Certificate ID.

Request Parameters

Table 4-1557 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-1558 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1559 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1560 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1561 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1562 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3093",
  "error_msg" : "App quota c900c5612dbe451bb43cbcc49cfaf2f3 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```


Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.27.7 Modifying an SSL Certificate

Function

This API is used to modify an SSL certificate.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/certificates/{certificate_id}

Table 4-1563 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
certificate_id	Yes	String	Certificate ID.

Request Parameters

Table 4-1564 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1565 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Certificate name. It can contain 4 to 50 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
cert_content	Yes	String	Certificate content.
private_key	Yes	String	Certificate private key.
type	No	String	Certificate scope. Default: global
instance_id	No	String	Gateway ID. This parameter is required if type is set to instance.
trusted_root_ca	No	String	Trusted root certificate (CA).
algorithm_type	No	String	Certificate algorithm type: • RSA • ECC • SM2
cert_content_sign	No	String	Signature certificate content. This parameter is mandatory only when algorithm_type is set to SM2. Maximum: 8092
private_key_sign	No	String	Signature private key content. This parameter is mandatory only when algorithm_type is set to SM2. Maximum: 8092

Response Parameters

Status code: 200

Table 4-1566 Response body parameters

Parameter	Type	Description
id	String	Certificate ID.
name	String	Certificate name.
type	String	Certificate type. • global: Global certificate. • instance: Gateway certificate.
instance_id	String	Gateway ID. • If type is set to global, the default value is common. • If type is set to instance, a gateway ID is displayed.
project_id	String	Project ID.
common_name	String	Domain name.
san	Array of strings	SAN domain name.
not_after	String	Expiration time.
signature_algorithm	String	Signature algorithm.
create_time	String	Creation time.
update_time	String	Update time.
is_has_trusted_root_ca	Boolean	Whether a trusted root certificate (CA) exists. The value is true if trusted_root_ca exists in the bound certificate. Default: false
algorithm_type	String	Certificate algorithm type: • RSA • ECC • SM2
version	Integer	Version.
organization	Array of strings	Company or organization.

Parameter	Type	Description
organizational_unit	Array of strings	Department.
locality	Array of strings	City.
state	Array of strings	State or province.
country	Array of strings	Country or region.
not_before	String	Effective time.
serial_number	String	Serial number.
issuer	Array of strings	Issuer.

Status code: 400**Table 4-1567** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1568** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1569** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1570 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1571** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Modifying an SSL certificate

```
{
  "name" : "cert_demo",
  "private_key" : "-----BEGIN PRIVATE KEY-----THIS IS YOUR PRIVATE KEY-----END PRIVATE KEY-----\\n",
  "cert_content" : "-----BEGIN CERTIFICATE-----THIS IS YOUR CERT CONTENT-----END CERTIFICATE-----\\n"
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "a27be832f2e9441c8127fe48e3b5ac67",
  "name" : "cert_demo",
  "common_name" : "apigtest.example.com",
  "san" : [ "apigtest.example.com", "*.san.com" ],
  "version" : 3,
  "organization" : [ "XX" ],
  "organizational_unit" : [ "IT" ],
  "locality" : [ "XX" ],
  "state" : [ "XX" ],
  "country" : [ "XX" ],
  "not_before" : "2019-06-01T00:00:00Z",
  "not_after" : "2031-08-16T06:36:13Z",
  "serial_number" : "13010",
  "issuer" : [ "XXSSL Inc" ],
  "signature_algorithm" : "SHA256-RSA",
  "create_time" : "2021-08-20T02:03:53Z",
  "update_time" : "2021-08-20T02:03:53Z",
  "algorithm_type" : "RSA"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.3325",
  "error_msg" : "The dictionary name already exists"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3093",
  "error_msg" : "App quota c900c5612dbe451bb43cbcc49cfaf2f3 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.27.8 Binding an SSL Certificate to a Domain Name

Function

This API is used to bind an SSL certificate to a domain name. For gateways with custom inbound ports, the same domain name is bound to a certificate at the same time. Enabling or disabling client verification takes effect for different ports of the same domain name.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/certificates/{certificate_id}/domains/attach

Table 4-1572 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
certificate_id	Yes	String	Certificate ID.

Request Parameters

Table 4-1573 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1574 Request body parameters

Parameter	Mandatory	Type	Description
domains	Yes	Array of AttachOrDetachDomainInfo objects	Domain names the certificate is bound to or unbound from.

Table 4-1575 AttachOrDetachDomainInfo

Parameter	Mandatory	Type	Description
domain	Yes	String	Domain name.
instance_ids	No	Array of strings	Gateway IDs.
verified_client_certificate_enabled	No	Boolean	Whether to enable client certificate verification. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist.

Response Parameters

Status code: 204

OK

Status code: 400

Table 4-1576 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1577 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1578 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 404**Table 4-1579** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1580** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Binding an SSL certificate to a domain name

```
{
  "domains": [ {
    "domain": "apigtest.example.com",
    "instance_ids": [ "f0fa1789-3b76-433b-a787-9892951c620e", "7d39549681c54d968ec2910da9da95cd" ]
  } ]
}
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2012",
  "error_msg": "Invalid parameter value,parameterName:domain_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
}
```

```
{
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3020",
  "error_msg": "The URL domain does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
204	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.27.9 Unbinding an SSL Certificate from a Domain Name

Function

This API is used to unbind an SSL certificate from a domain name. For gateways with custom inbound ports, the same domain name will be unbound from the certificate at the same time.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/certificates/{certificate_id}/domains/detach

Table 4-1581 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
certificate_id	Yes	String	Certificate ID.

Request Parameters

Table 4-1582 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1583 Request body parameters

Parameter	Mandatory	Type	Description
domains	Yes	Array of AttachOrDetachDomainInfo objects	Domain names the certificate is bound to or unbound from.

Table 4-1584 AttachOrDetachDomainInfo

Parameter	Mandatory	Type	Description
domain	Yes	String	Domain name.
instance_ids	No	Array of strings	Gateway IDs.

Parameter	Mandatory	Type	Description
verified_client_certificate_enabled	No	Boolean	Whether to enable client certificate verification. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist.

Response Parameters

Status code: 204

OK

Status code: 400

Table 4-1585 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1586 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1587 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1588 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1589 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Unbinding an SSL certificate from a domain name

```
{
  "domains": [ {
    "domain": "apigtest.example.com",
    "instance_ids": [ "f0fa1789-3b76-433b-a787-9892951c620e", "7d39549681c54d968ec2910da9da95cd" ]
  } ]
}
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2012",
  "error_msg": "Invalid parameter value,parameterName:domain_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3020",
  "error_msg" : "The URL domain does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.27.10 Querying Domain Names of an SSL Certificate

Function

This API is used to query the domain names to which an SSL certificate has been bound.

Calling MethodFor details, see [Calling APIs](#).**URI**

GET /v2/{project_id}/apigw/certificates/{certificate_id}/attached-domains

Table 4-1590 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
certificate_id	Yes	String	Certificate ID.

Table 4-1591 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
url_domain	No	String	Independent domain name.

Request Parameters

Table 4-1592 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1593 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
bound_domains	Array of UrlDomainRefInfo objects	Bound domain names.

Table 4-1594 UrlDomainRefInfo

Parameter	Type	Description
url_domain	String	Custom domain name.
id	String	Domain ID.
status	Integer	CNAME resolution status. • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
min_ssl_version	String	Minimum SSL version supported.
is_http_redirect_to_https	Boolean	Whether to enable HTTP redirection to HTTPS. The value false means disable and true means enable. The default value is false. Default: false
verified_client_certificate_enabled	Boolean	Whether to enable client certificate verification. This parameter is available only when a certificate is bound. It is enabled by default if trusted_root_ca exists, and disabled if trusted_root_ca does not exist. Default: false

Parameter	Type	Description
ingress_http_port	Integer	Inbound HTTP port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 80. Other valid ports must be included in the HTTP inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 80 is used. If this parameter is set, https_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ingress_https_port	Integer	Inbound HTTPS port bound to the domain name. -1 indicates that no port is available and the protocol is not supported. In this case, you can use the default port 443. Other valid ports must be included in the HTTPS inbound ports of the gateway. The value ranges from 1024 to 49151. When creating a domain name, if this parameter is not set, the default port 443 is used. If this parameter is set, http_port must be set. If both http_port and https_port need to use the default port, leave both parameters blank. If this parameter is not specified when you modify the domain name, the port number remains unchanged. Minimum: -1 Maximum: 49151
ssl_id	String	Certificate ID.
ssl_name	String	Certificate name.
api_group_id	String	API group ID.
api_group_name	String	API group name.

Parameter	Type	Description
instance_id	String	Gateway ID.

Status code: 400**Table 4-1595** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1596** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1597** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1598** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "bound_domains" : [ {
    "id" : "b9be707660c5406394f8973e087bae20",
    "url_domain" : "apigtest.example.com",
    "status" : 3,
    "min_ssl_version" : "TLSv1.1",
    "ssl_id" : "a27be832f2e9441c8127fe48e3b5ac67",
    "ssl_name" : "cert_demo",
    "instance_id" : "f0fa1789-3b76-433b-a787-9892951c620e",
    "api_group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
    "api_group_name" : "default"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:dict_name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.28 Plug-in Management

4.28.1 Creating a Plug-in

Function

Plug-in information.

- Plug-in names must be unique.
- Plug-ins must be bound to an API and take effect immediately for the API after binding.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/plugins

Table 4-1599 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1600 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1601 Request body parameters

Parameter	Mandatory	Type	Description
plugin_name	Yes	String	Plug-in name. Enter 3 to 255 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
plugin_type	Yes	String	Plug-in type • cors: Cross-origin resource sharing. • set_resp_headers: HTTP response header management. • kafka_log: Kafka log push. • breaker: Circuit breaker. • rate_limit: Request throttling. • third_auth: Third-party authentication. • proxy_cache: Response cache. • proxy_mirror: request mirroring
plugin_scope	Yes	String	Plug-in scope. global: Visible to all gateways.

Parameter	Mandatory	Type	Description
plugin_content	Yes	String	Plug-in content in JSON format. For details, see the model definition. - CorsPluginContent - SetRespHeadersContent - KafkaLogContent - BreakerContent - RateLimitContent - ThirdAuthContent - ProxyCacheContent - ProxyMirrorContent Maximum: 65535
remark	No	String	Plug-in description, with a maximum of 255 characters. Maximum: 255

Response Parameters

Status code: 201

Table 4-1602 Response body parameters

Parameter	Type	Description
plugin_id	String	Plug-in ID.
plugin_name	String	Plug-in name. Start with a letter, and include only letters, digits, hyphens (-), and underscores(_). (3 to 255 characters)
plugin_type	String	Plug-in type • cors: Cross-origin resource sharing. • set_resp_headers: HTTP response header management. • kafka_log: Kafka log push. • breaker: Circuit breaker. • rate_limit: Request throttling. • third_auth: Third-party authentication. • proxy_cache: Response cache. • proxy_mirror: request mirroring

Parameter	Type	Description
plugin_scope	String	Plug-in scope. global: Visible to all gateways.
plugin_content	String	Plug-in content in JSON format. For details, see the model definition. - CorsPluginContent - SetRespHeadersContent - KafkaLogContent - BreakerContent - RateLimitContent - ThirdAuthContent - ProxyCacheContent - ProxyMirrorContent Maximum: 65535
remark	String	Plug-in description, with a maximum of 255 characters. Maximum: 255
create_time	String	Creation time.
update_time	String	Update time.

Status code: 400**Table 4-1603** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1604** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1605 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1606** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1607** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

- Creating a CORS plug-in

```
{
  "plugin_name" : "CORS",
  "plugin_type" : "cors",
  "plugin_scope" : "global",
  "plugin_content" : "{\"allow_origin\": \"*\", \"allow_methods\": \"GET,POST,PUT\", \"allow_headers\": \"Content-Type,Accept,Accept-Ranges,Cache-Control\", \"expose_headers\": \"X-Request-Id,X-Apig-Latency\", \"max_age\": 172800, \"allow_credentials\": true}\",
  \"remark\" : \"Cross-origin resource sharing\"
}
```

- Creating an HTTP response header plug-in

```
{
  "plugin_name" : "HTTP Response Header Plug-in",
  "plugin_type" : "set_resp_headers",
  "plugin_scope" : "global",
  "plugin_content" : "{\"response_headers\": [{\"name\": \"x-demo\", \"value_type\": \"custom_value\", \"value\": \"sss\", \"action\": \"append\"}]}\",
  \"remark\" : \"HTTP response header management\"
}
```

- Creating a request throttling plug-in

```
{
  "plugin_name" : "Request Throttling Plug-in",
  "plugin_type" : "rate_limit",
}
```



```
"plugin_scope" : "global",
"plugin_content" : "{\\"scope\\":\\"basic\\",\\"default_time_unit\\":\\"minute\\",\\
\\default_interval\\":1,\\"api_limit\\":50,\\"app_limit\\":0,\\"user_limit\\":0,\\"ip_limit\\":0,\\
\\algorithm\\":\\"counter\\",\\"specials\\":[],\\"parameters\\":[],\\"rules\\":[]}",
"remark" : "Request throttling"
}
```

- Creating a Kafka log push plug-in

```
{
  "plugin_name" : "Kafka Log Plug-in",
  "plugin_type" : "kafka_log",
  "plugin_scope" : "app",
  "plugin_content" : "{\\"broker_list\\":[\\\"0.0.0.0:11\\\"],\\"topic\\":\\"topic\\",\\"key\\":\\"\\",\\
\\max_retry_count\\":0,\\"retry_backoff\\":1,\\"sasl_config\\":{\\"security_protocol\\":\\
\\PLAINTEXT\\",\\"sasl_mechanisms\\":\\"PLAIN\\",\\"sasl_username\\":\\"\\",\\"sasl_password\\
\\":\\"\\",\\"ssl_ca_content\\":\\"\\",\\"meta_config\\":{\\"system\\":{\\"start_time\\":true,\\
\\request_id\\":true,\\"client_ip\\":true,\\"api_id\\":false,\\"user_name\\":false,\\"app_id\\":false,\\
\\access_model1\\":false,\\"request_time\\":true,\\"http_status\\":true,\\"server_protocol\\
\\":false,\\"scheme\\":true,\\"request_method\\":true,\\"host\\":false,\\"api_uri_mode\\":false,\\
\\uri\\":false,\\"request_size\\":false,\\"response_size\\":false,\\"upstream_uri\\":false,\\
\\upstream_addr\\":true,\\"upstream_status\\":true,\\"upstream_connect_time\\":false,\\
\\upstream_header_time\\":false,\\"upstream_response_time\\":true,\\"all_upstream_response_time\\
\\":false,\\"region_id\\":false,\\"auth_type\\":false,\\"http_x_forwarded_for\\":true,\\
\\http_user_agent\\":true,\\"error_type\\":true,\\"access_model2\\":false,\\"inner_time\\":false,\\
\\proxy_protocol_vni\\":false,\\"proxy_protocol_vpc_id\\":false,\\"proxy_protocol_addr\\":false,\\
\\body_bytes_sent\\":false,\\"api_name\\":false,\\"app_name\\":false,\\"provider_app_id\\":false,\\
\\provider_app_name\\":false,\\"custom_data_log01\\":false,\\"custom_data_log02\\":false,\\
\\custom_data_log03\\":false,\\"custom_data_log04\\":false,\\"custom_data_log05\\":false,\\
\\custom_data_log06\\":false,\\"custom_data_log07\\":false,\\"custom_data_log08\\":false,\\
\\custom_data_log09\\":false,\\"custom_data_log10\\":false,\\"response_source\\":false},\\
\\call_data\\":{\\"log_request_header\\":false,\\"request_header_filter\\":\\"\\",\\
\\log_request_query_string\\":false,\\"request_query_string_filter\\":\\"\\",\\"log_request_body\\
\\":false,\\"log_response_header\\":false,\\"response_header_filter\\":\\"\\",\\"log_response_body\\
\\":false,\\"custom_authorizer\\":{\\"frontend\\":[],\\"backend\\":[]}}}",
  "remark" : "Kafka log push"
}
```

- Creating a circuit breaker plug-in

```
{
  "plugin_name" : "Circuit Breaker Plug-in",
  "plugin_type" : "breaker",
  "plugin_scope" : "app",
  "plugin_content" : "{\\"breaker_condition\\":{\\"breaker_type\\":\\"timeout\\",\\"breaker_mode\\
\\":\\"counter\\",\\"unhealthy_condition\\":\\"\\",\\"unhealthy_threshold\\":30,\\
\\min_call_threshold\\":20,\\"unhealthy_percentage\\":51,\\"time_window\\":15,\\
\\open_breaker_time\\":15},\\"downgrade_default\\":null,\\"downgrade_parameters\\":null,\\
\\downgrade_rules\\":null,\\"scope\\":\\"basic\\"}",
  "remark" : "Circuit breaker"
}
```

- Creating a third-party authentication plug-in

```
{
  "plugin_name" : "Third-Party Authentication Plug-in",
  "remark" : "This is a third-party authentication plug-in that contains a rule expression whitelist.",
  "plugin_type" : "third_auth",
  "plugin_scope" : "global",
  "plugin_content" : "{\\"auth_request\\":{\\"method\\":\\"POST\\",\\"protocol\\":\\"HTTP\\",\\
\\url_domain\\":\\"xxx.xxx.xxx.xxx:1234\\",\\"timeout\\":10,\\"path\\":\\"/check\\",\\
\\vpc_channel_enabled\\":false,\\"vpc_channel_info\\":{\\"vpc_proxy_host\\":\\"abc.com\\",\\
\\vpc_id\\":\\"3c113f40a54a40369ceb1eb1409a32ee\\"},\\"identities\\":{\\"headers\\":{\\"name\\":\\
\\token\\"},\\"query\\":{\\"name\\":\\"user\\"},\\"carry_body\\":{\\"enabled\\":true,\\
\\max_body_size\\":10000},\\"carry_path_enabled\\":false,\\"return_resp_body_enabled\\":true,\\
\\carry_resp_headers\\":{\\"x-message-result\\"},\\"simple_auth_mode_enabled\\":false,\\
\\match_auth\\":{\\"key\\":\\"x-message-result\\",\\"value\\":\\"success\\"},\\"rule_enabled\\
\\":true,\\"rule_type\\":\\"allow\\",\\"parameters\\":{\\"value\\":\\"reqPath\\",\\"type\\":\\
\\path\\",\\"name\\":\\"reqPath\\"},\\"value\\":\\"method\\",\\"type\\":\\"method\\",\\
\\name\\":\\"method\\"},\\"value\\":\\"Host\\",\\"type\\":\\"header\\",\\"name\\":\\"Host\\
\\"},\\"rules\\":{\\"match_regex\\":\\"[\\\"OR\\\",\\\"reqPath\\\",\\\"~\\\",\\
\\\"/xxl-job-admin/*\\\",\\\"reqPath\\\",\\\"==\\\",\\\"/app/leave/infor/v1/
addLeaveLnfor\\\",\\\"reqPath\\\",\\\"==\\\",\\\"/api/v1/charge/home/\\
\\\"}"}"
```

- Creating a response cache plug-in

- Creating a request mirroring plug-in

Example Responses

Status code: 201

OK

- ```
"plugin_content" : "{\\"response_headers\\":{\\"name\\":\\"x-demo\\",\\"value_type\\":\\"custom_value\\",\\"value\\":\\"sss\\",\\"action\\":\\"append\\"}}",
"remark" : "HTTP response header management",
"create_time" : "2022-11-02T12:31:23.353Z",
"update_time" : "2022-11-02T12:31:23.353Z"
}
```
- ```
{
  "plugin_id" : "9642ff2b9a86481689ca9d28babcf7f",
  "plugin_name" : "Request Throttling Plug-in",
  "plugin_type" : "rate_limit",
  "plugin_scope" : "global",
  "plugin_content" : "{\\"scope\\":\\"basic\\",\\"default_time_unit\\":\\"minute\\",\\"default_interval\\":1,\\"api_limit\\":50,\\"app_limit\\":0,\\"user_limit\\":0,\\"ip_limit\\":0,\\"algorithm\\":\\"counter\\",\\"specials\\":[],\\"parameters\\":[],\\"rules\\":[]}",
  "remark" : "Request throttling",
  "create_time" : "2022-11-02T12:31:23.353Z",
  "update_time" : "2022-11-02T12:31:23.353Z"
}
```
 - ```
{
 "plugin_id" : "92284ece6ec7466da2c2ac2416f46d5d",
 "plugin_name" : "Kafka Log Plug-in",
 "plugin_type" : "kafka_log",
 "plugin_scope" : "app",
 "plugin_content" : "{\\"broker_list\\":["0.0.0.0:11"],\\"topic\\":\\"topic\\",\\"key\\":\\"\\",\\"max_retry_count\\":0,\\"retry_backoff\\":1,\\"sas_config\\":{\\"security_protocol\\":\\"PLAINTEXT\\",\\"sas_mechanisms\\":\\"PLAIN\\",\\"sas_username\\":\\"\\",\\"sas_password\\":\\"\\",\\"ssl_ca_content\\":\\"\\",\\"meta_config\\":{\\"system\\":{\\"start_time\\":true,\\"request_id\\":true,\\"client_ip\\":true,\\"api_id\\":false,\\"user_name\\":false,\\"app_id\\":false,\\"access_model1\\":false,\\"request_time\\":true,\\"http_status\\":true,\\"server_protocol\\":false,\\"scheme\\":true,\\"request_method\\":true,\\"host\\":false,\\"api_uri_mode\\":false,\\"uri\\":false,\\"request_size\\":false,\\"response_size\\":false,\\"upstream_uri\\":false,\\"upstream_addr\\":true,\\"upstream_status\\":true,\\"upstream_connect_time\\":false,\\"upstream_header_time\\":false,\\"upstream_response_time\\":true,\\"all_upstream_response_time\\":false,\\"region_id\\":false,\\"auth_type\\":false,\\"http_x_forwarded_for\\":true,\\"http_user_agent\\":true,\\"error_type\\":true,\\"access_model2\\":false,\\"inner_time\\":false,\\"proxy_protocol_vni\\":false,\\"proxy_protocol_vpce_id\\":false,\\"proxy_protocol_addr\\":false,\\"body_bytes_sent\\":false,\\"api_name\\":false,\\"app_name\\":false,\\"provider_app_id\\":false,\\"provider_app_name\\":false,\\"custom_data_log01\\":false,\\"custom_data_log02\\":false,\\"custom_data_log03\\":false,\\"custom_data_log04\\":false,\\"custom_data_log05\\":false,\\"custom_data_log06\\":false,\\"custom_data_log07\\":false,\\"custom_data_log08\\":false,\\"custom_data_log09\\":false,\\"custom_data_log10\\":false,\\"response_source\\":false},\\"call_data\\":{\\"log_request_header\\":false,\\"request_header_filter\\":\\"\\",\\"log_request_query_string\\":false,\\"request_query_string_filter\\":\\"\\",\\"log_request_body\\":false,\\"log_response_header\\":false,\\"response_header_filter\\":\\"\\",\\"log_response_body\\":false},\\"custom_authORIZER\\":{\\"frontend\\":[],\\"backend\\":[]}}",
 "remark" : "Kafka log push",
 "create_time" : "2022-11-02T12:31:23.353Z",
 "update_time" : "2022-11-02T12:31:23.353Z"
}
```
  - ```
{
  "plugin_id" : "8b5253ed723c4a878e7b8532c08763b4",
  "plugin_name" : "Circuit Breaker Plug-in",
  "plugin_type" : "breaker",
  "plugin_scope" : "app",
  "plugin_content" : "{\\"breaker_condition\\":{\\"breaker_type\\":\\"timeout\\",\\"breaker_mode\\":\\"counter\\",\\"unhealthy_condition\\":\\"\\",\\"unhealthy_threshold\\":30,\\"min_call_threshold\\":20,\\"unhealthy_percentage\\":51,\\"time_window\\":15,\\"open_breaker_time\\":15},\\"downgrade_default\\":null,\\"downgrade_parameters\\":null,\\"downgrade_rules\\":null,\\"scope\\":\\"basic\\"}",
  "remark" : "Circuit breaker",
  "create_time" : "2022-11-02T12:31:23.353Z",
  "update_time" : "2022-11-02T12:31:23.353Z"
}
```
 - ```
{
 "plugin_id" : "235d97683439437585aff06020059720",
 "plugin_name" : "Third-Party Authentication Plug-in",
 "plugin_type" : "third_auth",

```

```
{
 "plugin_id": "d5bf25cf31e04e888907b8ad72563f45",
 "plugin_name": "Response Cache Plug-in",
 "plugin_type": "proxy_cache",
 "plugin_scope": "global",
 "plugin_content": "{\\\"cache_key\\\": {\\\"system_params\\\": [\\\"$context.sourceIp\\\", \\\"$context.requestId\\\"]}, \\\"parameters\\\": [\\\"demo_parameter\\\"], \\\"headers\\\": [\\\"demo_header\\\"]}, \\\"cache_http_status_and_ttl\\\": [{\\\"http_status\\\": 200}, {\\\"ttl\\\": 300}], \\\"http_status\\\": 300}, {\\\"ttl\\\": 200}], \\\"client_cache_control\\\": {\\\"mode\\\": \\\"apps\\\"}, \\\"datas\\\": [\\\"demo_app_id_1, demo_app_id_2\\\"]}, \\\"cacheable_headers\\\": [\\\"demo_cacheable_headers_1, demo_cacheable_headers_2\\\"]}",
 "remark": "This is a response cache plug-in.",
 "create_time": "2024-03-18T12:31:23.353Z",
 "update_time": "2024-03-18T12:31:23.353Z"
}
```

## Bad Request

```
{
 "error_code" : "APIG.3326",
```

```
{
 "error_msg" : "The plugin name already exists"
}
```

**Status code: 401**

Unauthorized

```
{
 "error_code" : "APIG.1002",
 "error_msg" : "Incorrect token or token resolution failed"
}
```

**Status code: 403**

Forbidden

```
{
 "error_code" : "APIG.1005",
 "error_msg" : "No permissions to request this method"
}
```

**Status code: 404**

Not Found

```
{
 "error_code" : "APIG.3030",
 "error_msg" : "The instance does not exist;id:f0fa1789-3b76-433b-a787-9892951c620ec"
}
```

**Status code: 500**

Internal Server Error

```
{
 "error_code" : "APIG.9999",
 "error_msg" : "System error"
}
```

## Status Codes

| Status Code | Description           |
|-------------|-----------------------|
| 201         | OK                    |
| 400         | Bad Request           |
| 401         | Unauthorized          |
| 403         | Forbidden             |
| 404         | Not Found             |
| 500         | Internal Server Error |

## Error Codes

See [Error Codes](#).

## 4.28.2 Modifying a Plug-in

### Function

This API is used to modify a plug-in.

- Plug-in names must be unique.
- The plug-in type and scope cannot be modified.

### Calling Method

For details, see [Calling APIs](#).

### URI

PUT /v2/{project\_id}/apigw/instances/{instance\_id}/plugins/{plugin\_id}

**Table 4-1608** Path Parameters

| Parameter   | Mandatory | Type   | Description                                                                                  |
|-------------|-----------|--------|----------------------------------------------------------------------------------------------|
| project_id  | Yes       | String | Project ID. For details about how to obtain it, see <a href="#">Obtaining a Project ID</a> . |
| instance_id | Yes       | String | Gateway ID, which can be obtained from the gateway information on the APIG console.          |
| plugin_id   | Yes       | String | Plug-in ID.                                                                                  |

### Request Parameters

**Table 4-1609** Request header parameters

| Parameter    | Mandatory | Type   | Description                                                                                                                                        |
|--------------|-----------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | Yes       | String | User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token. |

**Table 4-1610** Request body parameters

| Parameter      | Mandatory | Type   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|-----------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| plugin_name    | Yes       | String | Plug-in name. Enter 3 to 255 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.                                                                                                                                                                                                                                                                                                                                                                            |
| plugin_type    | Yes       | String | Plug-in type <ul style="list-style-type: none"><li>• cors: Cross-origin resource sharing.</li><li>• set_resp_headers: HTTP response header management.</li><li>• kafka_log: Kafka log push.</li><li>• breaker: Circuit breaker.</li><li>• rate_limit: Request throttling.</li><li>• third_auth: Third-party authentication.</li><li>• proxy_cache: Response cache.</li><li>• proxy_mirror: request mirroring</li></ul>                                                                             |
| plugin_scope   | Yes       | String | Plug-in scope. global: Visible to all gateways.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| plugin_content | Yes       | String | Plug-in content in JSON format. For details, see the model definition. <ul style="list-style-type: none"><li>- <a href="#">CorsPluginContent</a></li><li>- <a href="#">SetRespHeadersContent</a></li><li>- <a href="#">KafkaLogContent</a></li><li>- <a href="#">BreakerContent</a></li><li>- <a href="#">RateLimitContent</a></li><li>- <a href="#">ThirdAuthContent</a></li><li>- <a href="#">ProxyCacheContent</a></li><li>- <a href="#">ProxyMirrorContent</a></li></ul> Maximum: <b>65535</b> |
| remark         | No        | String | Plug-in description, with a maximum of 255 characters.<br>Maximum: <b>255</b>                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Response Parameters

Status code: 200

**Table 4-1611** Response body parameters

| Parameter      | Type   | Description                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| plugin_id      | String | Plug-in ID.                                                                                                                                                                                                                                                                                                                                                                                                            |
| plugin_name    | String | Plug-in name. Start with a letter, and include only letters, digits, hyphens (-), and underscores(_). (3 to 255 characters)                                                                                                                                                                                                                                                                                            |
| plugin_type    | String | Plug-in type <ul style="list-style-type: none"><li>• cors: Cross-origin resource sharing.</li><li>• set_resp_headers: HTTP response header management.</li><li>• kafka_log: Kafka log push.</li><li>• breaker: Circuit breaker.</li><li>• rate_limit: Request throttling.</li><li>• third_auth: Third-party authentication.</li><li>• proxy_cache: Response cache.</li><li>• proxy_mirror: request mirroring</li></ul> |
| plugin_scope   | String | Plug-in scope. global: Visible to all gateways.                                                                                                                                                                                                                                                                                                                                                                        |
| plugin_content | String | Plug-in content in JSON format. For details, see the model definition. <ul style="list-style-type: none"><li>- CorsPluginContent</li><li>- SetRespHeadersContent</li><li>- KafkaLogContent</li><li>- BreakerContent</li><li>- RateLimitContent</li><li>- ThirdAuthContent</li><li>- ProxyCacheContent</li><li>- ProxyMirrorContent</li></ul> Maximum: <b>65535</b>                                                     |
| remark         | String | Plug-in description, with a maximum of 255 characters.<br>Maximum: <b>255</b>                                                                                                                                                                                                                                                                                                                                          |
| create_time    | String | Creation time.                                                                                                                                                                                                                                                                                                                                                                                                         |
| update_time    | String | Update time.                                                                                                                                                                                                                                                                                                                                                                                                           |



**Status code: 400****Table 4-1612** Response body parameters

| Parameter  | Type   | Description    |
|------------|--------|----------------|
| error_code | String | Error code.    |
| error_msg  | String | Error message. |

**Status code: 401****Table 4-1613** Response body parameters

| Parameter  | Type   | Description    |
|------------|--------|----------------|
| error_code | String | Error code.    |
| error_msg  | String | Error message. |

**Status code: 403****Table 4-1614** Response body parameters

| Parameter  | Type   | Description    |
|------------|--------|----------------|
| error_code | String | Error code.    |
| error_msg  | String | Error message. |

**Status code: 404****Table 4-1615** Response body parameters

| Parameter  | Type   | Description    |
|------------|--------|----------------|
| error_code | String | Error code.    |
| error_msg  | String | Error message. |

**Status code: 500****Table 4-1616** Response body parameters

| Parameter  | Type   | Description |
|------------|--------|-------------|
| error_code | String | Error code. |

| Parameter | Type   | Description    |
|-----------|--------|----------------|
| error_msg | String | Error message. |

## Example Requests

- Updating a CORS plug-in

```
{
 "plugin_name" : "CORS",
 "plugin_type" : "cors",
 "plugin_scope" : "global",
 "plugin_content" : "{ \"allow_origin\" : \"*\", \"allow_methods\" : \"GET,POST,PUT\", \"allow_headers\" : \"Content-Type,Accept,Accept-Ranges,Cache-Control\", \"expose_headers\" : \"X-Request-Id,X-Apig-Latency\", \"max_age\" : 172800, \"allow_credentials\" : true }",
 "remark" : "Cross-origin resource sharing"
}
```

- Updating an HTTP response header plug-in

```
{
 "plugin_name" : "HTTP Response Header Plug-in",
 "plugin_type" : "set_resp_headers",
 "plugin_scope" : "global",
 "plugin_content" : "{ \"response_headers\" : { \"name\" : \"x-demo\", \"value_type\" : \"custom_value\", \"value\" : \"sss\", \"action\" : \"append\" } }",
 "remark" : "HTTP response header management"
}
```

- Updating a request throttling plug-in

```
{
 "plugin_name" : "Request Throttling Plug-in",
 "plugin_type" : "rate_limit",
 "plugin_scope" : "global",
 "plugin_content" : "{ \"scope\" : \"basic\", \"default_time_unit\" : \"minute\", \"default_interval\" : 1, \"api_limit\" : 50, \"app_limit\" : 0, \"user_limit\" : 0, \"ip_limit\" : 0, \"algorithm\" : \"counter\", \"specials\" : [], \"parameters\" : [], \"rules\" : [] }",
 "remark" : "Request throttling"
}
```

- Updating a Kafka log push plug-in

```
{
 "plugin_name" : "Kafka Log Plug-in",
 "plugin_type" : "kafka_log",
 "plugin_scope" : "app",
 "plugin_content" : "{ \"broker_list\" : [\"0.0.0.0:11\"], \"topic\" : \"topic\", \"key\" : \"\", \"max_retry_count\" : 0, \"retry_backoff\" : 1, \"sas_config\" : { \"security_protocol\" : \"PLAINTEXT\", \"sas_mechanisms\" : \"PLAIN\", \"sas_username\" : \"\", \"sas_password\" : \"\", \"ssl_ca_content\" : \"\", \"meta_config\" : { \"system\" : { \"start_time\" : true, \"request_id\" : true, \"client_ip\" : true, \"api_id\" : false, \"user_name\" : false, \"app_id\" : false, \"access_model1\" : false, \"request_time\" : true, \"http_status\" : true, \"server_protocol\" : false, \"scheme\" : true, \"request_method\" : true, \"host\" : false, \"api_uri_mode\" : false, \"uri\" : false, \"request_size\" : false, \"response_size\" : false, \"upstream_uri\" : false, \"upstream_addr\" : true, \"upstream_status\" : true, \"upstream_connect_time\" : false, \"upstream_header_time\" : false, \"upstream_response_time\" : true, \"all_upstream_response_time\" : false, \"region_id\" : false, \"auth_type\" : false, \"http_x_forwarded_for\" : true, \"http_user_agent\" : true, \"error_type\" : true, \"access_model2\" : false, \"inner_time\" : false, \"proxy_protocol_vni\" : false, \"proxy_protocol_vpce_id\" : false, \"proxy_protocol_addr\" : false, \"body_bytes_sent\" : false, \"api_name\" : false, \"app_name\" : false, \"provider_app_id\" : false, \"provider_app_name\" : false, \"custom_data_log01\" : false, \"custom_data_log02\" : false, \"custom_data_log03\" : false, \"custom_data_log04\" : false, \"custom_data_log05\" : false, \"custom_data_log06\" : false, \"custom_data_log07\" : false, \"custom_data_log08\" : false, \"custom_data_log09\" : false, \"custom_data_log10\" : false, \"response_source\" : false }, \"call_data\" : { \"log_request_header\" : false, \"request_header_filter\" : \"\", \"log_request_query_string\" : false, \"request_query_string_filter\" : \"\", \"log_request_body\" : false, \"log_response_header\" : false, \"response_header_filter\" : \"\", \"log_response_body\" : false, \"custom_authorizer\" : { \"frontend\" : [], \"backend\" : [] } } } }",
 "remark" : "Kafka log push plug-in"
}
```

- Updating a circuit breaker plug-in

- Updating a third-party authentication plug-in

- Updating the response cache plug-in

```
{
 "plugin_name": "Response Cache Plug-in",
 "remark": "This is a response cache plug-in.",
 "plugin_type": "proxy_cache",
 "plugin_scope": "global",
 "plugin_content": "{\\\"cache_key\\\": {\\\"system_params\\\": [\\\"$context.sourceIp\\\"], \\\"$context.requestId\\\"}, \\\"parameters\\\": [\\\"demo_parameter\\\"], \\\"headers\\\": [\\\"demo_header\\\"]}, \\\"cache_http_status_and_ttl\\\": {\\\"http_status\\\": [200], \\\"ttl\\\": 300}, {\\\"http_status\\\": [300], \\\"ttl\\\": 200}}, \\\"client_cache_control\\\": {\\\"mode\\\": \\\"apps\\\"}, \\\"datas\\\": [\\\"demo_app_id_1, demo_app_id_2\\\"]}, \\\"cacheable_headers\\\": [\\\"demo_cacheable_headers_1, demo_cacheable_headers_2\\\"]}"
}
```

- Updating a request mirroring plug-in

```
{
 "plugin_name": "Request mirroring plug-in",
 "remark": "This is a request mirroring plug-in.",
 "plugin_type": "proxy_mirror",
 "plugin_scope": "global",
 "plugin_content": "{\"protocol\":\"http\",\"host\":\"xxx.xxx.xxx.xxx:1234\",\"path\":\"/test/\",\"path_concat_mode\":\"replace\",\"sample_ratio\":\"1\",\"timeout\":\"5000\",\"mirror_request_body_enabled\": true}"
}
```

## Example Responses

Status code: 200

OK

- ```
{
  "plugin_id": "5b729aa252764739b3s237ef0d66dc63",
  "plugin_name": "CORS Plug-in",
  "plugin_type": "cors",
  "plugin_scope": "global",
  "plugin_content": "{\"allow_origin\":\"*\",\"allow_methods\":\"GET,POST,PUT\",\"allow_headers\":\"Content-Type,Accept,Accept-Ranges,Cache-Control\",\"expose_headers\":\"X-Request-Id,X-Apig-Latency\",\"max_age\":\"172800\",\"allow_credentials\": true}",
  "remark": "Cross-origin resource sharing.",
  "create_time": "2020-11-02T12:31:23.353Z",
  "update_time": "2020-11-02T12:31:23.353Z"
}
```
- ```
{
 "plugin_id": "8a688dce7d0c45cf84edac3d7b071769",
 "plugin_name": "HTTP Response Header Plug-in",
 "plugin_type": "set_resp_headers",
 "plugin_scope": "global",
 "plugin_content": "{\"response_headers\":{\"name\":\"x-demo\",\"value\":\"sss\"},\"action\":\"append\"}",
 "remark": "HTTP response header management",
 "create_time": "2022-11-02T12:31:23.353Z",
 "update_time": "2022-11-02T12:31:23.353Z"
}
```
- ```
{
  "plugin_id": "9642ff2b9a86481689ca9d28babcf7f",
  "plugin_name": "Request Throttling Plug-in",
  "plugin_type": "rate_limit",
  "plugin_scope": "global",
  "plugin_content": "{\"scope\":\"basic\",\"default_time_unit\":\"minute\",\"default_interval\":\"1\",\"api_limit\":\"50\",\"app_limit\":\"0\",\"user_limit\":\"0\",\"ip_limit\":\"0\",\"algorithm\":\"counter\",\"specials\":{},\"parameters\":{},\"rules\":{}}",
  "remark": "Request throttling",
  "create_time": "2022-11-02T12:31:23.353Z",
  "update_time": "2022-11-02T12:31:23.353Z"
}
```
- ```
{
 "plugin_id": "92284ece6ec7466da2c2ac2416f46d5d",
 "plugin_name": "Kafka Log Plug-in",
 "plugin_type": "kafka_log",
 "plugin_scope": "app",
 "plugin_content": "{\"broker_list\":\"0.0.0.0:11\",\"topic\":\"topic\",\"key\":\"key\",\"max_retry_count\":\"0\",\"retry_backoff\":\"1\",\"sas_config\":{\"security_protocol\":\"PLAINTEXT\",\"sas_mechanisms\":\"PLAIN\",\"sas_username\":\"\",\"sas_password\":\"\",\"ssl_ca_content\":\"\",\"meta_config\":{\"system\":{\"start_time\":true,\"request_id\":true,\"client_ip\":true,\"api_id\":false,\"user_name\":false,\"app_id\":false,\"access_model\":false,\"request_time\":true,\"http_status\":true,\"server_protocol\":false,\"scheme\":true,\"request_method\":true,\"host\":false,\"api_uri_mode\":false,\"uri\":false,\"request_size\":false,\"response_size\":false,\"upstream_uri\":false,\"upstream_addr\":true,\"upstream_status\":true,\"upstream_connect_time\":false,\"
```

```
{
 "plugin_id": "8b5253ed723c4a878e7b8532c08763b4",
 "plugin_name": "Circuit Breaker Plug-in",
 "plugin_type": "breaker",
 "plugin_scope": "app",
 "plugin_content": "{\n \"breaker_condition\": \"{\n \"breaker_type\": \"timeout\",\n \"breaker_mode\": \"counter\",\n \"unhealthy_condition\": \"unhealthy_threshold:30,min_call_threshold:20,unhealthy_percentage:51,time_window:15,open_breaker_time:15,downgrade_default:null,downgrade_parameters:null,downgrade_rules:{\n \"scope\": \"basic\"\n }\n }\",\n \"remark\": \"Circuit breaker\",\n \"create_time\": \"2022-11-02T12:31:23.353Z\",\n \"update_time\": \"2022-11-02T12:31:23.353Z\"\n }",
 "create_time": "2022-11-02T12:31:23.353Z",
 "update_time": "2022-11-02T12:31:23.353Z"
}
```

```
{
 "plugin_id": "235d97683439437585aff06020059720",
 "plugin_name": "Third-Party Authentication Plug-in",
 "plugin_type": "third_auth",
 "plugin_scope": "global",
 "plugin_content": "{\n \"auth_request\": {\n \"method\": \"POST\",\n \"protocol\": \"HTTP\",\n \"url_domain\": \"xxx.xxx.xxx.xxx:1234\",\n \"path\": \"/check\",\n \"timeout\": 10,\n \"vpc_channel_enabled\": false,\n \"vpc_channel_info\": null,\n \"identities\": {\n \"headers\": {\n \"name\": \"token\"\n },\n \"queries\": null,\n \"carry_body\": {\n \"enabled\": true,\n \"max_body_size\": 10000,\n \"carry_path_enabled\": false,\n \"return_resp_body_enabled\": true,\n \"carry_resp_headers\": {\n \"x-message-result\": \"simple_auth_mode_enabled\": false,\n \"match_auth\": {\n \"key\": \"x-message-result\",\n \"value\": \"success\",\n \"parameters\": {\n \"type\": \"path\",\n \"name\": \"reqPath\",\n \"value\": \"reqPath\",\n \"type\": \"method\",\n \"name\": \"method\",\n \"value\": \"method\",\n \"type\": \"header\",\n \"name\": \"Host\",\n \"value\": \"Host\"\n },\n \"rules\": {\n \"rule_name\": \"allow2\",\n \"match_regex\": \"OR\",\n \"reqPath\": \"~\",\n \"xxl-job-admin\": \"reqPath\", \"=/\", \"/app/leave/infor/v1/addLeaveLnfor\", \"reqPath\", \"=/\", \"/api/v1/charge/home/modifyChargeSync\", \"reqPath\", \"=/\", \"/app/mweb/campaign/api/v1/getActivityConfig\", \"reqPath\", \"=/\", \"/mp/vehicle/owner/home\", \"reqPath\", \"=/\", \"/app/mweb/campaign/api/v1/getTime\", \"reqPath\", \"=/\", \"/api/c-showroom-service/v1/vehicleDetails/upload\", \"reqPath\", \"~/\", \"~/operation-charging-bff/carOwnerRights/certificate/*\", \"reqPath\", \"~/\", \"~/api/2c/v1/sales-bff/*\", \"reqPath\", \"=/\", \"~/api/2c/v1/vehicleDetails/upload\", \"reqPath\", \"~/\", \"~/operation-admin/*\", \"reqPath\", \"=/\", \"/app/settings/api/v1/receiveCk\", \"reqPath\", \"=/\", \"/api/vehicle/relative/yTSendVehicleControl.json\", \"reqPath\", \"=/\", \"/appoint/getAppointmentByTestDrive\", \"reqPath\", \"=/\", \"/api/evd/callbackEvdPay\", \"reqPath\", \"=/\", \"/api/evd/callbackEvdOrder\", \"reqPath\", \"=/\", \"/api/evd/callbackEvdCoupon\", \"reqPath\", \"=/\", \"/api/evd/getUserToken\", \"reqPath\", \"=/\", \"/api/task/busTriggerTaskEvent.json\", \"reqPath\", \"=/\", \"/datacenter-log-center/api/trackApi/commonAdd.json\" }\n },\n \"rule_type\": \"allow\",\n \"rule_enabled\": true,\n \"custom_forbid_limit\": 100,\n \"auth_downgrade_enable\": false,\n \"remark\": \"This is a third-party authentication plug-in that contains a rule expression blacklist\",\n \"create_time\": \"2023-05-06T06:54:59.296181801Z\"\n }",
 "create_time": "2023-05-06T06:54:59.296181801Z",
 "update_time": "2023-05-06T06:54:59.296181801Z"
}
```

- ```
"update_time" : "2023-05-06T07:07:18.369017889Z"
}
```
- ```
{
 "plugin_id" : "d5bf25cf31e04e888907b8ad72563f45",
 "plugin_name" : "Response Cache Plug-in",
 "plugin_type" : "proxy_cache",
 "plugin_scope" : "global",
 "plugin_content" : "{\\\"cache_key\\\": {\\\"system_params\\\": [\\\"$context.sourceIp\\\", \\\"$context.requestId\\\"]}, \\\"parameters\\\": [\\\"demo_parameter\\\"], \\\"headers\\\": [\\\"demo_header\\\"]}, \\\"cache_http_status_and_ttl\\\": {\\\"http_status\\\": [200], \\\"ttl\\\": 300}, {\\\"http_status\\\": [300], \\\"ttl\\\": 200}}, \\\"client_cache_control\\\": {\\\"mode\\\": \\\"apps\\\", \\\"datas\\\": [\\\"demo_app_id_1, demo_app_id_2\\\"]}, \\\"cacheable_headers\\\": [\\\"demo_cacheable_headers_1, demo_cacheable_headers_2\\\"]}, \\\"remark\\\": \\\"This is a response cache plug-in.\\\", \\\"create_time\\\": \\\"2024-03-18T12:31:23.353Z\\\", \\\"update_time\\\": \\\"2024-03-18T12:31:23.353Z\\\"
}
```
  - ```
{
  "plugin_id" : "d5bf25cf31e04e888907b8ad72563f45",
  "plugin_name" : "Request mirroring plug-in",
  "plugin_type" : "proxy_mirror",
  "plugin_scope" : "global",
  "plugin_content" : "{\\\"protocol\\\": \\\"http\\\", \\\"host\\\": \\\"xxx.xxx.xxx.xxx:1234\\\", \\\"path\\\": \\\"/test\\\", \\\"path_concat_mode\\\": \\\"replace\\\", \\\"sample_ratio\\\": 1, \\\"timeout\\\": 5000, \\\"mirror_request_body_enabled\\\": true}, \\\"remark\\\": \\\"This is a request mirroring plug-in.\\\", \\\"create_time\\\": \\\"2024-03-18T12:31:23.353Z\\\", \\\"update_time\\\": \\\"2024-03-18T12:31:23.353Z\\\"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.3326",
  "error_msg" : "The plugin name already exists"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3068",
  "error_msg" : "Plugin b294018ee0554156a875b3513e02e5b9 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.28.3 Deleting a Plug-in

Function

This API is used to delete a plug-in.

- Before deleting a plug-in, unbind it from all APIs.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}

Table 4-1617 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
plugin_id	Yes	String	Plug-in ID.

Request Parameters

Table 4-1618 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-1619 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1620 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1621** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1622** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 409**Table 4-1623** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1624** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 400**

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3068",
  "error_msg" : "Plugin b294018ee0554156a875b3513e02e5b9 does not exist"
}
```

Status code: 409

Conflict

```
{
  "error_code" : "APIG.3462",
  "error_msg" : "The plugin has been attached to the APIs and cannot perform the current operation"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
409	Conflict
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.28.4 Querying Plug-ins

Function

This API is used to query details about a group of plug-ins that meet specified conditions.

- Pagination query
- Query by plug-in type
- Query by plug-in scope
- Query by plug-in ID
- Fuzzy query by plug-in name

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/plugins

Table 4-1625 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1626 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
plugin_type	No	String	Plug-in type.
plugin_scope	No	String	Plug-in scope.
plugin_id	No	String	Plug-in ID.
plugin_name	No	String	Plug-in name, which can be used for fuzz query.
precise_search	No	String	Parameter name for exact match. Plug-in name is supported.

Request Parameters

Table 4-1627 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1628 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
plugins	Array of PluginInfo objects	Plug-ins.

Table 4-1629 PluginInfo

Parameter	Type	Description
plugin_id	String	Plug-in ID.
plugin_name	String	Plug-in name. Start with a letter, and include only letters, digits, hyphens (-), and underscores(_). (3 to 255 characters)
plugin_type	String	Plug-in type • cors: Cross-origin resource sharing. • set_resp_headers: HTTP response header management. • kafka_log: Kafka log push. • breaker: Circuit breaker. • rate_limit: Request throttling. • third_auth: Third-party authentication. • proxy_cache: Response cache. • proxy_mirror: request mirroring
plugin_scope	String	Plug-in scope. global: Visible to all gateways.

Parameter	Type	Description
plugin_content	String	Plug-in content in JSON format. For details, see the model definition. - CorsPluginContent - SetRespHeadersContent - KafkaLogContent - BreakerContent - RateLimitContent - ThirdAuthContent - ProxyCacheContent - ProxyMirrorContent Maximum: 65535
remark	String	Plug-in description, with a maximum of 255 characters. Maximum: 255
create_time	String	Creation time.
update_time	String	Update time.

Status code: 400**Table 4-1630** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1631** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1632 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1633** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total": 1,
  "size": 1,
  "plugins": [ {
    "plugin_id": "5b729aa252764739b3s237ef0d66dc63",
    "plugin_name": "CORS",
    "plugin_type": "cors",
    "plugin_scope": "global",
    "plugin_content": "{ \"allow_origin\": \"*\", \"allow_methods\": \"GET,POST,PUT\", \"allow_headers\": \"Content-Type,Accept,Accept-Ranges,Cache-Control\", \"expose_headers\": \"X-Request-Id,X-Apig-Latency\", \"max_age\": 172800, \"allow_credentials\": true }",
    "remark": "Cross-origin resource sharing",
    "create_time": "2022-11-02T12:31:23.353Z",
    "update_time": "2022-11-02T12:31:23.353Z"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2012",
  "error_msg": "Invalid parameter value,parameterName:plugin_name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.28.5 Querying Plug-in Details

Function

This API is used to query the details of a plug-in.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}

Table 4-1634 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
plugin_id	Yes	String	Plug-in ID.

Request Parameters

Table 4-1635 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1636 Response body parameters

Parameter	Type	Description
plugin_id	String	Plug-in ID.
plugin_name	String	Plug-in name. Start with a letter, and include only letters, digits, hyphens (-), and underscores(_). (3 to 255 characters)

Parameter	Type	Description
plugin_type	String	Plug-in type • cors: Cross-origin resource sharing. • set_resp_headers: HTTP response header management. • kafka_log: Kafka log push. • breaker: Circuit breaker. • rate_limit: Request throttling. • third_auth: Third-party authentication. • proxy_cache: Response cache. • proxy_mirror: request mirroring
plugin_scope	String	Plug-in scope. global: Visible to all gateways.
plugin_content	String	Plug-in content in JSON format. For details, see the model definition. - CorsPluginContent - SetRespHeadersContent - KafkaLogContent - BreakerContent - RateLimitContent - ThirdAuthContent - ProxyCacheContent - ProxyMirrorContent Maximum: 65535
remark	String	Plug-in description, with a maximum of 255 characters. Maximum: 255
create_time	String	Creation time.
update_time	String	Update time.

Status code: 400**Table 4-1637** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1638** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1639** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1640** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1641** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "plugin_id" : "5b729aa252764739b3s237ef0d66dc63",
  "plugin_name" : "CORS",
  "plugin_type" : "cors",
  "plugin_scope" : "global",
  "plugin_content" : "{\"allow_origin\": \"*\", \"allow_methods\": \"GET,POST,PUT\", \"allow_headers\": \"Content-Type,Accept,Accept-Ranges,Cache-Control\", \"expose_headers\": \"X-Request-Id,X-Apig-Latency\", \"max_age\": 172800, \"allow_credentials\": true}",
  "remark" : "Cross-origin resource sharing",
  "create_time" : "2022-11-02T12:31:23.353Z",
  "update_time" : "2022-11-02T12:31:23.353Z"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3068",
  "error_msg" : "Plugin b294018ee0554156a875b3513e02e5b9 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.28.6 Binding a Plug-in to APIs

Function

This API is used to bind a plug-in to APIs.

- Plug-ins can be bound only to published APIs.
- Plug-ins take effect immediately after binding.
- Plug-ins take effect immediately after being modified.
- An API can be bound with only one plug-in of the same type. Binding another plug-in will overwrite the previous one.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attach

Table 4-1642 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
plugin_id	Yes	String	Plug-in ID.

Request Parameters

Table 4-1643 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1644 Request body parameters

Parameter	Mandatory	Type	Description
env_id	Yes	String	ID of the environment for binding to the API.
api_ids	Yes	Array of strings	IDs of bound APIs. Array Length: 1 - 500

Response Parameters

Status code: 201

Table 4-1645 Response body parameters

Parameter	Type	Description
attached_plugins	Array of PluginApiAttachInfo objects	Bound plug-ins.

Table 4-1646 PluginApiAttachInfo

Parameter	Type	Description
plugin_attach_id	String	Plug-in binding record ID.
plugin_id	String	Plug-in ID.
plugin_name	String	Plug-in name. Start with a letter, and include only letters, digits, hyphens (-), and underscores(_). (3 to 255 characters)
plugin_type	String	Plug-in type • cors: Cross-origin resource sharing. • set_resp_headers: HTTP response header management. • kafka_log: Kafka log push. • breaker: Circuit breaker. • rate_limit: Request throttling. • third_auth: Third-party authentication. • proxy_cache: Response cache. • proxy_mirror: request mirroring
plugin_scope	String	Plug-in scope. global: Visible to all gateways.
env_id	String	ID of the environment for binding to the API.
env_name	String	Name of the environment for binding to the API.
api_id	String	API ID.
api_name	String	API name.
attached_time	String	Binding time.

Status code: 400**Table 4-1647** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1648 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1649** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1650** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1651** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Binding an API with plug-ins

```
{
  "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "api_ids" : [ "8aa097b00e9843efabc9c593d11b769d" ]
}
```


Example Responses

Status code: 201

OK

```
{
  "attached_plugins": [ {
    "plugin_attach_id": "8aa097b00e9843efacb9c593d11b769e",
    "plugin_id": "5b729aa252764739b3s237ef0d66dc63",
    "plugin_name": "CORS",
    "plugin_type": "cors",
    "plugin_scope": "global",
    "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "env_name": "RELEASE",
    "api_id": "8aa097b00e9843efabc9c593d11b769d",
    "api_name": "api_name",
    "attached_time": "2022-11-02T12:31:23.353Z"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2012",
  "error_msg": "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3068",
  "error_msg": "Plugin b294018ee0554156a875b3513e02e5b9 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
201	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.28.7 Binding an API with Plug-ins

Function

This API is used to bind an API with plug-ins.

- Plug-ins can be bound only to published APIs.
- Plug-ins take effect immediately after binding.
- Plug-ins take effect immediately after being modified.
- An API can be bound with only one plug-in of the same type. Binding another plug-in will overwrite the previous one.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/apis/{api_id}/plugins/attach

Table 4-1652 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
api_id	Yes	String	API ID.

Request Parameters

Table 4-1653 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1654 Request body parameters

Parameter	Mandatory	Type	Description
env_id	Yes	String	ID of the environment for binding to the API.
plugin_ids	Yes	Array of strings	IDs of bound plug-ins. Array Length: 1 - 500

Response Parameters

Status code: 201

Table 4-1655 Response body parameters

Parameter	Type	Description
attached_plugins	Array of PluginApiAttachment objects	Bound plug-ins.

Table 4-1656 PluginApiAttachInfo

Parameter	Type	Description
plugin_attach_id	String	Plug-in binding record ID.
plugin_id	String	Plug-in ID.
plugin_name	String	Plug-in name. Start with a letter, and include only letters, digits, hyphens (-), and underscores(_). (3 to 255 characters)
plugin_type	String	Plug-in type • cors: Cross-origin resource sharing. • set_resp_headers: HTTP response header management. • kafka_log: Kafka log push. • breaker: Circuit breaker. • rate_limit: Request throttling. • third_auth: Third-party authentication. • proxy_cache: Response cache. • proxy_mirror: request mirroring
plugin_scope	String	Plug-in scope. global: Visible to all gateways.
env_id	String	ID of the environment for binding to the API.
env_name	String	Name of the environment for binding to the API.
api_id	String	API ID.
api_name	String	API name.
attached_time	String	Binding time.

Status code: 400**Table 4-1657** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1658 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1659** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1660** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1661** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Binding a plug-in to APIs

```
{
  "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "plugin_ids" : [ "5b729aa252764739b3s237ef0d66dc63" ]
}
```

Example Responses

Status code: 201

OK

```
{
  "attached_plugins": [ {
    "plugin_attach_id": "8aa097b00e9843efacb9c593d11b769e",
    "plugin_id": "5b729aa252764739b3s237ef0d66dc63",
    "plugin_name": "CORS",
    "plugin_type": "cors",
    "plugin_scope": "global",
    "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "env_name": "RELEASE",
    "api_id": "8aa097b00e9843efabc9c593d11b769d",
    "api_name": "api_name",
    "attached_time": "2022-11-02T12:31:23.353Z"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2012",
  "error_msg": "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3068",
  "error_msg": "Plugin b294018ee0554156a875b3513e02e5b9 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
201	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.28.8 Unbinding a Plug-in from All APIs

Function

This API is used to unbind a plug-in from all APIs to which it has been bound.

- The unbinding takes effect immediately.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/detach

Table 4-1662 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
plugin_id	Yes	String	Plug-in ID.

Request Parameters

Table 4-1663 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1664 Request body parameters

Parameter	Mandatory	Type	Description
env_id	Yes	String	ID of the environment for binding to the API.
api_ids	Yes	Array of strings	IDs of bound APIs. Array Length: 1 - 500

Response Parameters

Status code: 204

OK

Status code: 400

Table 4-1665 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1666 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1667** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1668** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1669** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Unbinding a plug-in from all APIs to which it has been bound

```
{
  "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "api_ids" : [ "8aa097b00e9843efabc9c593d11b769d" ]
}
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3068",
  "error_msg" : "Plugin b294018ee0554156a875b3513e02e5b9 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.28.9 Unbinding an API's Plug-ins

Function

This API is used to unbind an API's plug-ins.

- The unbinding takes effect immediately.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/apis/{api_id}/plugins/detach

Table 4-1670 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
api_id	Yes	String	API ID.

Request Parameters

Table 4-1671 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1672 Request body parameters

Parameter	Mandatory	Type	Description
env_id	Yes	String	ID of the environment for binding to the API.
plugin_ids	Yes	Array of strings	IDs of bound plug-ins. Array Length: 1 - 500

Response Parameters

Status code: 204

OK

Status code: 400

Table 4-1673 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1674 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1675 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1676 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1677 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Unbinding an API's plug-ins

```
{
  "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "plugin_ids" : [ "98df09fb-d459-4cbf-83a7-2b55ca6f3d5d" ]
}
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3068",
  "error_msg" : "Plugin b294018ee0554156a875b3513e02e5b9 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.28.10 Querying APIs Bound with a Plug-in

Function

This API is used to query the APIs to which a plug-in has been bound.

- Query APIs bound with a specified plug-in
- Pagination query
- Fuzzy query by API name
- APIs taken offline are also included.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attached-apis

Table 4-1678 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
plugin_id	Yes	String	Plug-in ID.

Table 4-1679 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
env_id	No	String	Environment ID.
api_name	No	String	API name.
api_id	No	String	API ID.
group_id	No	String	Group ID.
req_method	No	String	Request method.
req_uri	No	String	Request path.
tags	No	String	API tag. Multiple API tags can be specified. The relationship between multiple parameter values is OR. If this parameter is not specified, no filtering tag is specified. If this parameter is set to #no_tags#, APIs without tags are filtered. Minimum: 0 Maximum: 128

Request Parameters

Table 4-1680 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-1681** Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
apis	Array of PluginApiInfo objects	APIs bound to the plug-in.

Table 4-1682 PluginApiInfo

Parameter	Type	Description
api_id	String	API ID.
api_name	String	API name. Enter 3 to 255 characters, starting with a letter or digit. Only letters, digits, and these special characters are allowed: -_./:()
type	Integer	API type. 1: Public API. 2: Private API.

Parameter	Type	Description
req_protocol	String	API request protocol. • HTTP • HTTPS • BOTH: Both HTTP and HTTPS are supported. Default: HTTPS
req_method	String	Request method.
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications.
auth_type	String	API authentication mode. • NONE • APP • IAM • AUTHORIZER
match_mode	String	API matching mode. • SWA: Prefix match. • NORMAL: Exact match. Default value: NORMAL
remark	String	API description.
group_id	String	ID of the API group to which the API belongs.
group_name	String	Name of the API group to which the API belongs.
roma_app_id	String	Integration application ID for ROMA instances. This parameter can be left blank.

Parameter	Type	Description
env_id	String	ID of the environment for binding to the API.
env_name	String	Name of the environment for binding to the API.
publish_id	String	Publishing record ID.
plugin_attach_id	String	Plug-in binding record ID.
attached_time	String	Binding time.
tags	Array of strings	Tags bound to the API. The default quota is 10. You can contact technical support to adjust the quota. Minimum: 1 Maximum: 128 Array Length: 0 - 10

Status code: 400**Table 4-1683** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1684** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1685** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 404

Table 4-1686 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1687 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total": 1,
  "size": 1,
  "apis": [ {
    "api_id": "8aa097b00e9843efabc9c593d11b769d",
    "api_name": "Test_API",
    "type": 1,
    "req_protocol": "HTTP",
    "req_method": "GET",
    "req_uri": "/test",
    "auth_type": "IAM",
    "match_mode": "NORMAL",
    "remark": "API description.",
    "group_id": "b9be707660c5406394f8973e087bae20",
    "group_name": "DEFAULT",
    "roma_app_id": "",
    "plugin_attach_id": "8aa097b00e9843efabc9c593d11b769e",
    "publish_id": "4739b3s5b729aa2237ef0d66dc635276",
    "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "env_name": "RELEASE",
```

```
"attached_time" : "2022-11-02T12:31:23.353Z"
} ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support
documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3068",
  "error_msg" : "Plugin b294018ee0554156a875b3513e02e5b9 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

Status Code	Description
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.28.11 Querying Plug-ins Bound to an API

Function

This API is used to query the plug-ins bound to an API.

- Query plug-ins bound to a specified API
- Pagination query
- Fuzzy query by plug-in name

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apis/{api_id}/attached-plugins

Table 4-1688 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
api_id	Yes	String	API ID.

Table 4-1689 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
env_id	No	String	Environment ID.
plugin_name	No	String	Plug-in name.
plugin_id	No	String	Plug-in ID.
env_name	No	String	Environment name.
plugin_type	No	String	Plug-in type.

Request Parameters

Table 4-1690 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1691 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
plugins	Array of AttachedPluginInfo objects	Plug-ins bound to the API.

Table 4-1692 AttachedPluginInfo

Parameter	Type	Description
plugin_attach_id	String	Plug-in binding record ID.
plugin_id	String	Plug-in ID.
plugin_name	String	Plug-in name. Start with a letter, and include only letters, digits, hyphens (-), and underscores(_). (3 to 255 characters)
plugin_type	String	Plug-in type • cors: Cross-origin resource sharing. • set_resp_headers: HTTP response header management. • kafka_log: Kafka log push. • breaker: Circuit breaker. • rate_limit: Request throttling. • third_auth: Third-party authentication. • proxy_cache: Response cache. • proxy_mirror: request mirroring
plugin_scope	String	Plug-in scope. global: Visible to all gateways.
env_id	String	ID of the environment for binding to the API.
env_name	String	Name of the environment for binding to the API.
attached_time	String	Binding time.
plugin_content	String	Plug-in content in JSON format. Maximum: 65535

Parameter	Type	Description
remark	String	Plug-in description, with a maximum of 255 characters. Maximum: 255
create_time	String	Creation time.
update_time	String	Update time.

Status code: 400**Table 4-1693** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1694** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1695** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1696 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1697** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total": 1,
  "size": 1,
  "plugins": [ {
    "plugin_attach_id": "8aa097b00e9843efacb9c593d11b769e",
    "plugin_id": "5b729aa252764739b3s237ef0d66dc63",
    "plugin_name": "CORS",
    "plugin_type": "cors",
    "plugin_scope": "global",
    "plugin_content": "{ \"allow_origin\": \"*\", \"allow_methods\": \"GET,POST,PUT\", \"allow_headers\": \"Content-Type,Accept,Accept-Ranges,Cache-Control\", \"expose_headers\": \"X-Request-Id,X-Apig-Latency\", \"max_age\": 172800, \"allow_credentials\": true }",
    "remark": "Cross-origin resource sharing",
    "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "env_name": "RELEASE",
    "attached_time": "2022-11-02T12:31:23.353Z",
    "create_time": "2022-11-02T12:31:23.353Z",
    "update_time": "2022-11-02T12:31:23.353Z"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2012",
  "error_msg": "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "API 5f918d104dc84480a75166ba99efff21 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).

4.28.12 Querying APIs to Which a Plug-in Can Be Bound

Function

This API is used to query the APIs to which a plug-in can be bound.

- Pagination query
- Fuzzy query by API name
- APIs already bound with other plug-ins will also be returned.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attachable-apis

Table 4-1698 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
plugin_id	Yes	String	Plug-in ID.

Table 4-1699 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
env_id	Yes	String	Environment ID.
api_name	No	String	API name.
api_id	No	String	API ID.
group_id	No	String	Group ID.
req_method	No	String	Request method.
req_uri	No	String	Request path.
tags	No	String	API tag. Multiple API tags can be specified. The relationship between multiple parameter values is OR. If this parameter is not specified, no filtering tag is specified. If this parameter is set to #no_tags#, APIs without tags are filtered. Minimum: 0 Maximum: 128

Request Parameters

Table 4-1700 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1701 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
apis	Array of PluginApiInfo objects	APIs bound to the plug-in.

Table 4-1702 PluginApiInfo

Parameter	Type	Description
api_id	String	API ID.
api_name	String	API name. Enter 3 to 255 characters, starting with a letter or digit. Only letters, digits, and these special characters are allowed: -_./:()
type	Integer	API type. 1: Public API. 2: Private API.
req_protocol	String	API request protocol. - HTTP - HTTPS - BOTH: Both HTTP and HTTPS are supported. Default: HTTPS
req_method	String	Request method.

Parameter	Type	Description
req_uri	String	Request address, which can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications.
auth_type	String	API authentication mode. • NONE • APP • IAM • AUTHORIZER
match_mode	String	API matching mode. • SWA: Prefix match. • NORMAL: Exact match. Default value: NORMAL
remark	String	API description.
group_id	String	ID of the API group to which the API belongs.
group_name	String	Name of the API group to which the API belongs.
roma_app_id	String	Integration application ID for ROMA instances. This parameter can be left blank.
env_id	String	ID of the environment for binding to the API.
env_name	String	Name of the environment for binding to the API.
publish_id	String	Publishing record ID.
plugin_attach_id	String	Plug-in binding record ID.

Parameter	Type	Description
attached_time	String	Binding time.
tags	Array of strings	Tags bound to the API. The default quota is 10. You can contact technical support to adjust the quota. Minimum: 1 Maximum: 128 Array Length: 0 - 10

Status code: 400**Table 4-1703** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1704** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1705** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1706 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1707 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total": 1,
  "size": 1,
  "apis": [ {
    "api_id": "8aa097b00e9843efabc9c593d11b769d",
    "api_name": "Test_API",
    "type": 1,
    "req_protocol": "HTTP",
    "req_method": "GET",
    "req_uri": "/test",
    "auth_type": "IAM",
    "match_mode": "NORMAL",
    "remark": "API description.",
    "group_id": "b9be707660c5406394f8973e087bae20",
    "group_name": "DEFAULT",
    "roma_app_id": "",
    "plugin_attach_id": "8aa097b00e9843efabc9c593d11b769e",
    "publish_id": "4739b3s5b729aa2237ef0d66dc635276",
    "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "env_name": "RELEASE",
    "attached_time": "2020-11-02T12:31:23.353Z"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2012",
  "error_msg": "Invalid parameter value,parameterName:instance_id. Please refer to the support
```



```
documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3068",
  "error_msg" : "Plugin b294018ee0554156a875b3513e02e5b9 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.28.13 Querying Plug-ins That Can Be Bound to an API

Function

This API is used to query the plug-ins that can be bound to a specified API.

- Pagination query
- Fuzzy query by plug-in name

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apis/{api_id}/attachable-plugins

Table 4-1708 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
api_id	Yes	String	API ID.

Table 4-1709 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
env_id	No	String	Environment ID.
plugin_name	No	String	Plug-in name.
plugin_type	No	String	Plug-in type.
plugin_id	No	String	Plug-in ID.

Request Parameters

Table 4-1710 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1711 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
plugins	Array of PluginInfo objects	Plug-ins.

Table 4-1712 PluginInfo

Parameter	Type	Description
plugin_id	String	Plug-in ID.
plugin_name	String	Plug-in name. Start with a letter, and include only letters, digits, hyphens (-), and underscores(_). (3 to 255 characters)
plugin_type	String	Plug-in type • cors: Cross-origin resource sharing. • set_resp_headers: HTTP response header management. • kafka_log: Kafka log push. • breaker: Circuit breaker. • rate_limit: Request throttling. • third_auth: Third-party authentication. • proxy_cache: Response cache. • proxy_mirror: request mirroring
plugin_scope	String	Plug-in scope. global: Visible to all gateways.
plugin_content	String	Plug-in content in JSON format. For details, see the model definition. - CorsPluginContent - SetRespHeadersContent - KafkaLogContent - BreakerContent - RateLimitContent - ThirdAuthContent - ProxyCacheContent - ProxyMirrorContent Maximum: 65535
remark	String	Plug-in description, with a maximum of 255 characters. Maximum: 255
create_time	String	Creation time.
update_time	String	Update time.

Status code: 400

Table 4-1713 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1714** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1715** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1716** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1717** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "plugins" : [ {
    "plugin_id" : "5b729aa252764739b3s237ef0d66dc63",
    "plugin_name" : "CORS",
    "plugin_type" : "cors",
    "plugin_scope" : "global",
    "plugin_content" : "{\"allow_origin\": \"*\", \"allow_methods\": \"GET,POST,PUT\", \"allow_headers\": \"Content-Type,Accept,Accept-Ranges,Cache-Control\", \"expose_headers\": \"X-Request-Id,X-Apig-Latency\", \"max_age\": 172800, \"allow_credentials\": true}\",
    "remark" : "Cross-origin resource sharing",
    "create_time" : "2022-11-02T12:31:23.353Z",
    "update_time" : "2022-11-02T12:31:23.353Z"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "API 5f918d104dc84480a75166ba99efff21 does not exist"
}
```

Status code: 500

Internal Server Error

```
{  
  "error_code" : "APIG.9999",  
  "error_msg" : "System error"  
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

Credential Management

4.29.1 Creating an App

Function

An app is an identity for accessing an API. An app can call the APIs to which it has been authorized.

This API is used to create an app.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/apps

Table 4-1718 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1719 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1720 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	App name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
remark	No	String	App description. It cannot exceed 255 characters.
app_key	No	String	AppKey, which can contain 8 to 200 characters, starting with a letter or digit. Only letters, digits, hyphens (-), and underscores (_) are allowed.
app_secret	No	String	Secret, which can contain 8 to 128 characters, starting with a letter or digit. Only letters, digits, and the following special characters are allowed: _-!@#\$\$%

Response Parameters

Status code: 201

Table 4-1721 Response body parameters

Parameter	Type	Description
id	String	ID.
name	String	Name.
remark	String	Description.
creator	String	Creator of the app. • USER: The app is created by an API user. • MARKET: The app is allocated by KooGallery. The value MARKET is currently not supported.
update_time	String	Update time.
app_key	String	AppKey.
app_secret	String	AppSecret.
register_time	String	Registration time.
status	Integer	Status. • 1: valid
app_type	String	App type. • apig: APIG app, which is not recommended. • roma: ROMA integration application. The default value is apig. Other types are not supported currently.
roma_app_type	String	ROMA application type. • subscription: subscription application • integration: integration application Currently, this parameter is not supported.

Status code: 400

Table 4-1722 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1723** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1724** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1725** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Creating an app

```
{
  "name" : "app_demo",
  "remark" : "Demo app"
}
```

Example Responses

Status code: 201

Created

```
{
  "creator" : "USER",
  "update_time" : "2020-08-03T13:09:13.122211909Z",
  "app_key" : "ee8f878c252747028f07eb116c2cd91b",
  "name" : "app_demo",
  "remark" : "Demo app",
  "id" : "356de8eb7a8742168586e5daf5339965",
  "app_secret" : "416*****ab8",
  "register_time" : "2020-08-03T13:09:13.122211659Z",
  "status" : 1,
  "app_type" : "apig"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized

Status Code	Description
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.29.2 Modifying an App

Function

This API is used to modify the information about an app. Only the name and remark parameters can be modified. If the function of customizing keys and secrets is enabled, app_key and app_secret can also be modified.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}

Table 4-1726 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.

Request Parameters

Table 4-1727 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1728 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	App name. It can contain 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
remark	No	String	App description. It cannot exceed 255 characters.
app_key	No	String	AppKey, which can contain 8 to 200 characters, starting with a letter or digit. Only letters, digits, hyphens (-), and underscores (_) are allowed.
app_secret	No	String	Secret, which can contain 8 to 128 characters, starting with a letter or digit. Only letters, digits, and the following special characters are allowed: _-!@#\$\$%

Response Parameters

Status code: 201**Table 4-1729** Response body parameters

Parameter	Type	Description
id	String	ID.
name	String	Name.
remark	String	Description.

Parameter	Type	Description
creator	String	Creator of the app. • USER: The app is created by an API user. • MARKET: The app is allocated by KooGallery. The value MARKET is currently not supported.
update_time	String	Update time.
app_key	String	AppKey.
app_secret	String	AppSecret.
register_time	String	Registration time.
status	Integer	Status. • 1: valid
app_type	String	App type. • apig: APIG app, which is not recommended. • roma: ROMA integration application. The default value is apig. Other types are not supported currently.
roma_app_type	String	ROMA application type. • subscription: subscription application • integration: integration application Currently, this parameter is not supported.

Status code: 400**Table 4-1730** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1731 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1732** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1733** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1734** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Modifying an app

```
{
  "name" : "app_demo",
  "remark" : "Demo app"
}
```

Example Responses

Status code: 201

OK

```
{
  "creator" : "USER",
  "update_time" : "2020-08-03T13:21:48.381148828Z",
  "app_key" : "ee8f878c252747028f07eb116c2cd91b",
  "name" : "app_demo",
  "remark" : "Demo app",
  "id" : "356de8eb7a8742168586e5daf5339965",
  "app_secret" : "416*****ab8",
  "register_time" : "2020-08-03T13:09:13",
  "status" : 1,
  "app_type" : "apig"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "App 356de8eb7a8742168586e5daf5339965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```


Status Codes

Status Code	Description
201	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.29.3 Deleting an App

Function

This API is used to delete an app.

Deleted apps cannot call APIs.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}

Table 4-1735 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.

Request Parameters

Table 4-1736 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400**Table 4-1737** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1738** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1739** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1740** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1741** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
}
```

```
{
  "error_msg" : "App 356de8eb7a8742168586e5daf5339965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.29.4 Resetting the AppSecret of an App

Function

This API is used to reset the AppSecret of an app.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/apps/secret/{app_id}

Table 4-1742 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.

Request Parameters

Table 4-1743 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1744 Request body parameters

Parameter	Mandatory	Type	Description
app_secret	No	String	Secret, which can contain 8 to 128 characters, starting with a letter or digit. Only letters, digits, and special characters (_-!@#\$\$%). To define an AppSecret, first enable the app_secret parameter.

Response Parameters

Status code: 200

Table 4-1745 Response body parameters

Parameter	Type	Description
id	String	ID.
name	String	Name.
remark	String	Description.

Parameter	Type	Description
creator	String	Creator of the app. • USER: The app is created by an API user. • MARKET: The app is allocated by KooGallery. The value MARKET is currently not supported.
update_time	String	Update time.
app_key	String	AppKey.
app_secret	String	AppSecret.
register_time	String	Registration time.
status	Integer	Status. • 1: valid
app_type	String	App type. • apig: APIG app, which is not recommended. • roma: ROMA integration application. The default value is apig. Other types are not supported currently.
roma_app_type	String	ROMA application type. • subscription: subscription application • integration: integration application Currently, this parameter is not supported.

Status code: 400**Table 4-1746** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1747 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1748** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1749** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1750** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Resetting secret

```
{  
  "app_secret" : "1ff*****9a4"  
}
```

Example Responses

Status code: 200

OK

```
{
  "creator" : "USER",
  "update_time" : "2020-08-03T14:12:43.038171689Z",
  "app_key" : "ee8f878c252747028f07eb116c2cd91b",
  "name" : "app_demo",
  "remark" : "Demo app",
  "id" : "356de8eb7a8742168586e5daf5339965",
  "app_secret" : "1ff*****9a4",
  "register_time" : "2020-08-03T13:09:13Z",
  "status" : 1,
  "app_type" : "apig"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "App 356de8eb7a8742168586e5daf5339965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK

Status Code	Description
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.29.5 Verifying an App

Function

This API is provided for users (excluding app owner) to check whether an app exists. Only the basic information, such as ID, name, and remark, of the app is displayed.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apps/validation/{app_id}

Table 4-1751 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.

Request Parameters

Table 4-1752 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1753 Response body parameters

Parameter	Type	Description
id	String	ID.
name	String	Name.
remark	String	Description.

Status code: 400

Table 4-1754 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1755 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-1756 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1757** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1758** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "name" : "app_demo",
  "remark" : "Demo app",
  "id" : "356de8eb7a8742168586e5daf5339965"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "App 356de8eb7a8742168586e5daf5339965 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.29.6 Querying App Details

Function

This API is used to query the details of an app.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}

Table 4-1759 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.

Request Parameters

Table 4-1760 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1761 Response body parameters

Parameter	Type	Description
id	String	ID.
name	String	Name.
remark	String	Description.

Parameter	Type	Description
creator	String	Creator of the app. • USER: The app is created by an API user. • MARKET: The app is allocated by KooGallery. The value MARKET is currently not supported.
update_time	String	Update time.
app_key	String	AppKey.
app_secret	String	AppSecret.
register_time	String	Registration time.
status	Integer	Status. • 1: valid
app_type	String	App type. • apig: APIG app, which is not recommended. • roma: ROMA integration application. The default value is apig. Other types are not supported currently.
roma_app_type	String	ROMA application type. • subscription: subscription application • integration: integration application Currently, this parameter is not supported.

Status code: 400**Table 4-1762** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1763 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1764** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1765** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1766** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{  
  "creator" : "USER",
```

```
"update_time" : "2020-08-03T13:09:13Z",  
"app_key" : "ee8f878c252747028f07eb116c2cd91b",  
"name" : "app_demo",  
"remark" : "Demo app",  
"id" : "356de8eb7a8742168586e5daf5339965",  
"app_secret" : "416*****ab8",  
"register_time" : "2020-08-03T13:09:13Z",  
"status" : 1,  
"app_type" : "apig"  
}
```

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2012",  
  "error_msg" : "Invalid parameter value,parameterName:id. Please refer to the support documentation"  
}
```

Status code: 401

Unauthorized

```
{  
  "error_code" : "APIG.1002",  
  "error_msg" : "Incorrect token or token resolution failed"  
}
```

Status code: 403

Forbidden

```
{  
  "error_code" : "APIG.1005",  
  "error_msg" : "No permissions to request this method"  
}
```

Status code: 404

Not Found

```
{  
  "error_code" : "APIG.3002",  
  "error_msg" : "App 356de8eb7a8742168586e5daf5339965 does not exist"  
}
```

Status code: 500

Internal Server Error

```
{  
  "error_code" : "APIG.9999",  
  "error_msg" : "System error"  
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized

Status Code	Description
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.29.7 Querying Apps

Function

This API is used to query apps.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apps

Table 4-1767 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1768 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
id	No	String	App ID.
name	No	String	App name.
status	No	Integer	App status.
app_key	No	String	AppKey.
creator	No	String	Creator of the app. • USER: The app is created by an API user. • MARKET: This parameter is not used currently.
precise_search	No	String	Parameter name (name) for exact matching.

Request Parameters

Table 4-1769 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1770 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
apps	Array of AppInfoWithBindNum objects	App list.

Table 4-1771 AppInfoWithBindNum

Parameter	Type	Description
id	String	ID.
name	String	Name.
remark	String	Description.
creator	String	Creator of the app. • USER: The app is created by an API user. • MARKET: The app is allocated by KooGallery. The value MARKET is currently not supported.
update_time	String	Update time.
app_key	String	AppKey.
app_secret	String	AppSecret.
register_time	String	Registration time.
status	Integer	Status. • 1: valid
app_type	String	App type. • apig: APIG app, which is not recommended. • roma: ROMA integration application. The default value is apig. Other types are not supported currently.

Parameter	Type	Description
roma_app_type	String	ROMA application type. • subscription: subscription application • integration: integration application Currently, this parameter is not supported.
bind_num	Integer	Number of bound APIs.

Status code: 400**Table 4-1772** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1773** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1774** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1775 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 2,
  "size" : 2,
  "apps" : [ {
    "bind_num" : 0,
    "creator" : "USER",
    "update_time" : "2020-08-03T13:09:13Z",
    "app_key" : "ee8f878c252747028f07eb116c2cd91b",
    "name" : "app_demo",
    "remark" : "Demo app",
    "id" : "356de8eb7a8742168586e5daf5339965",
    "app_secret" : "416*****ab8",
    "register_time" : "2020-08-03T13:09:13Z",
    "status" : 1,
    "app_type" : "apig"
  }, {
    "bind_num" : 3,
    "creator" : "USER",
    "update_time" : "2020-05-27T10:38:03.133586Z",
    "app_key" : "840b8b5b1efc4ec686639759c2c584da",
    "name" : "app_001",
    "id" : "9ed8b7fe84224de681e7d7a5587e76dc",
    "app_secret" : "0a4*****c6e",
    "register_time" : "2020-03-28T11:09:06Z",
    "status" : 1
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2011",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error CodesSee [Error Codes](#).**4.29.8 Creating an AppCode****Function**

This API is used to create an AppCode for an app for simple authentication.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes

Table 4-1776 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.

Request Parameters

Table 4-1777 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1778 Request body parameters

Parameter	Mandatory	Type	Description
app_code	Yes	String	AppCode value. It can contain 64 to 180 characters, starting with a letter, digit, plus sign (+), or slash (/). Only letters, digits, and the following special characters are allowed: +_!@#\$%-=

Response Parameters

Status code: 201

Table 4-1779 Response body parameters

Parameter	Type	Description
app_code	String	AppCode value. It can contain 64 to 180 characters, starting with a letter, digit, plus sign (+), or slash (/). Only letters, digits, and the following special characters are allowed: +_!@#\$\$%&-'/=
id	String	ID.
app_id	String	App ID.
create_time	String	Creation time.

Status code: 400**Table 4-1780** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1781** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1782** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-1783 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1784** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Creating an AppCode for simple authentication

```
{
  "app_code" : "GjOD3g80AABuuFeEJpVQADBLAjBh3UzC7W
+gr4VJBB5BtJ4fdVOQoSvoji3gFxUDb5pWBz9wUcw9+8/bFZ1B/4pq29wCMQC0pQWX6zTndljDEl99As1pw
+WntAU9xcq+ffagoH6zDpKUvdxV6Ezj8LcCcPZN6BU="
}
```

Example Responses

Status code: 201

Created

```
{
  "app_code" : "GjOD3g80AABuuFeEJpVQADBLAjBh3UzC7W
+gr4VJBB5BtJ4fdVOQoSvoji3gFxUDb5pWBz9wUcw9+8/bFZ1B/4pq29wCMQC0pQWX6zTndljDEl99As1pw
+WntAU9xcq+ffagoH6zDpKUvdxV6Ezj8LcCcPZN6BU=",
  "app_id" : "9ed8b7fe84224de681e7d7a5587e76dc",
  "id" : "32dc8ca22d1b4b9cb94022186880576b",
  "create_time" : "2020-07-24T02:37:24.835128293Z"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:app_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
}
```

```
{
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3004",
  "error_msg": "App 9ed8b7fe84224de681e7d7a5587e76dc does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.29.9 Generating an AppCode

Function

This API is used to generate a random AppCode.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes

Table 4-1785 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.

Request Parameters

Table 4-1786 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 201

Table 4-1787 Response body parameters

Parameter	Type	Description
app_code	String	AppCode value. It can contain 64 to 180 characters, starting with a letter, digit, plus sign (+), or slash (/). Only letters, digits, and the following special characters are allowed: +_!@#\$\$%&-'=
id	String	ID.
app_id	String	App ID.

Parameter	Type	Description
create_time	String	Creation time.

Status code: 400**Table 4-1788** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1789** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1790** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1791** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-1792 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 201

Created

```
{
  "app_code" : "fdc8d90a30174460a91ddacfa54d6f04c92e523a85cc4a1894f87cb13b6f572a",
  "app_id" : "9ed8b7fe84224de681e7d7a5587e76dc",
  "id" : "b3d34f746d0847fb95138670e10207ed",
  "create_time" : "2020-07-24T02:31:45.790909295Z"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:app_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3004",
  "error_msg" : "App 9ed8b7fe84224de681e7d7a5587e76dc does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.29.10 Deleting an AppCode

Function

This API is used to delete an AppCode. Deleted AppCodes cannot be used for simple authentication.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes/{app_code_id}

Table 4-1793 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.
app_code_id	Yes	String	AppCode ID.

Request Parameters

Table 4-1794 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-1795 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-1796 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1797** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1798** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1799** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:app_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```


Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3004",
  "error_msg" : "App 9ed8b7fe84224de681e7d7a5587e76dc does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error CodesSee [Error Codes](#).**4.29.11 Querying AppCode Details****Function**

This API is used to query the details of an AppCode created for an app for simple authentication.

Calling MethodFor details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes/{app_code_id}

Table 4-1800 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.
app_code_id	Yes	String	AppCode ID.

Request Parameters

Table 4-1801 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 201

Table 4-1802 Response body parameters

Parameter	Type	Description
app_code	String	AppCode value. It can contain 64 to 180 characters, starting with a letter, digit, plus sign (+), or slash (/). Only letters, digits, and the following special characters are allowed: +_!@#\$\$%&/'=
id	String	ID.

Parameter	Type	Description
app_id	String	App ID.
create_time	String	Creation time.

Status code: 400**Table 4-1803** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1804** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1805** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1806** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1807** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 201**

Created

```
{
  "app_code" : "fdc8d90a30174460a91ddacfa54d6f04c92e523a85cc4a1894f87cb13b6f572a",
  "app_id" : "9ed8b7fe84224de681e7d7a5587e76dc",
  "id" : "b3d34f746d0847fb95138670e10207ed",
  "create_time" : "2020-07-24T02:31:45Z"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:app_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3004",
  "error_msg" : "App 9ed8b7fe84224de681e7d7a5587e76dc does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.29.12 Querying AppCodes of an App

Function

This API is used to query the AppCodes of an app.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes

Table 4-1808 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.

Table 4-1809 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20

Request Parameters

Table 4-1810 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1811 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
app_codes	Array of AppCodeBaseInfo objects	AppCode list.

Table 4-1812 AppCodeBaseInfo

Parameter	Type	Description
app_code	String	AppCode value. It can contain 64 to 180 characters, starting with a letter, digit, plus sign (+), or slash (/). Only letters, digits, and the following special characters are allowed: +_!@#\$\$%-/=
id	String	ID.
app_id	String	App ID.
create_time	String	Creation time.

Status code: 400**Table 4-1813** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1814** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1815** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1816** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1817** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "total" : 2,
  "size" : 2,
  "app_codes" : [ {
    "app_code" : "GjOD3g80AABuuFeEJpVQADBlAjBh3UzC7W
+gr4VJBB5BtJ4fdVOQoSvoji3gFxUDb5pWBz9wUcw9+8/bFZ1B/4pq29wCMQC0pQWX6zTndljDEl99As1pw
+WntAU9xcq+ffagoH6zDpKUvdxV6Ezj8LcCcPZN6BU=",
    "app_id" : "9ed8b7fe84224de681e7d7a5587e76dc",
    "id" : "32dc8ca22d1b4b9cb94022186880576b",
    "create_time" : "2020-07-24T02:37:24Z"
  }, {
    "app_code" : "fdc8d90a30174460a91ddacfa54d6f04c92e523a85cc4a1894f87cb13b6f572a",
    "app_id" : "9ed8b7fe84224de681e7d7a5587e76dc",
```



```
{
  "id" : "b3d34f746d0847fb95138670e10207ed",
  "create_time" : "2020-07-24T02:31:45Z"
}]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:app_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3004",
  "error_msg" : "App 9ed8b7fe84224de681e7d7a5587e76dc does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

Status Code	Description
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.29.13 Querying Quotas Associated with a Credential

Function

This API is used to query quotas associated with a specified credential.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/bound-quota

Table 4-1818 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.

Request Parameters

Table 4-1819 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1820 Response body parameters

Parameter	Type	Description
app_quota_id	String	Credential quota ID.
name	String	Quota name. Enter 3 to 255 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
call_limits	Integer	Maximum number of times a credential quota can be called.
time_unit	String	Time unit. The options are SECOND, MINUTE, HOUR, and DAY.
time_interval	Integer	Time limit of a quota.
remark	String	Parameter description. Maximum: 255
reset_time	String	Time when the quota is reset for the first time. If this parameter is not specified, the time is calculated based on the first calling time by default.
create_time	String	Creation time.
bound_app_num	Integer	Number of applications bound to the quota policy.

Status code: 400

Table 4-1821 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401

Table 4-1822 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-1823** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-1824** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1825** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 200

OK

```
{  
  "app_quota_id" : "c900c5612dbe451bb43cbcc49cfaf2f3",
```

```
"name" : "ClientQuota_demo",
"call_limits" : 1000,
"time_unit" : "DAY",
"time_interval" : 1,
"remark" : "remark",
"reset_time" : "2020-09-20 00:00:00 +0000 +0000",
"create_time" : "2020-09-19T07:27:47Z",
"bound_app_num" : 0
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3002",
  "error_msg" : "App 98df09fb-d459-4cbf-83a7-2b55ca6f3d5d does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized

Status Code	Description
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.29.14 Configuring Access Control Settings for an App

Function

This API is used to configure access control settings for a credential.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-acl

Table 4-1826 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.

Request Parameters

Table 4-1827 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1828 Request body parameters

Parameter	Mandatory	Type	Description
app_acl_type	Yes	String	Type: • PERMIT (whitelist) • DENY (blacklist)
app_acl_values	Yes	Array of strings	Access control values. The values can be IP addresses, IP address ranges, or CIDR blocks. Use hyphens (-) to separate IP address segments.

Response Parameters

Status code: 201

Table 4-1829 Response body parameters

Parameter	Type	Description
app_id	String	App ID.
app_acl_type	String	Type: • PERMIT (whitelist) • DENY (blacklist)
app_acl_values	Array of strings	Access control values. The values can be IP addresses, IP address ranges, or CIDR blocks. Use hyphens (-) to separate IP address segments.

Status code: 400

Table 4-1830 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401**Table 4-1831** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-1832** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-1833** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1834** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

```
{
  "app_acl_type" : "PERMIT",
  "app_acl_values" : [ "192.168.0.1", "192.168.0.5-192.168.0.10", "192.168.0.100/28" ]
}
```

Example Responses

Status code: 201

Ok

```
{
  "app_id" : "9ed8b7fe84224de681e7d7a5587e76dc",
  "app_acl_type" : "PERMIT",
  "app_acl_values" : [ "192.168.0.1", "192.168.0.5-192.168.0.10", "192.168.0.100/28" ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:app_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3004",
  "error_msg" : "App 9ed8b7fe84224de681e7d7a5587e76dc does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Ok
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.29.15 Querying Access Control Details About an App

Function

This API is used to query the access control details about an app.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-acl

Table 4-1835 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.

Request Parameters

Table 4-1836 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-1837** Response body parameters

Parameter	Type	Description
app_id	String	App ID.
app_acl_type	String	Type: • PERMIT (whitelist) • DENY (blacklist)
app_acl_values	Array of strings	Access control values. The values can be IP addresses, IP address ranges, or CIDR blocks. Use hyphens (-) to separate IP address segments.

Status code: 400**Table 4-1838** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401

Table 4-1839 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403

Table 4-1840 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404

Table 4-1841 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500

Table 4-1842 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "app_id": "9ed8b7fe84224de681e7d7a5587e76dc",
```

```
"app_acl_type" : "PERMIT",  
"app_acl_values" : [ "192.168.0.1", "192.168.0.5-192.168.0.10", "192.168.0.100/28" ]  
}
```

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2012",  
  "error_msg" : "Invalid parameter value,parameterName:app_id. Please refer to the support documentation"  
}
```

Status code: 401

Unauthorized

```
{  
  "error_code" : "APIG.1002",  
  "error_msg" : "Incorrect token or token resolution failed"  
}
```

Status code: 403

Forbidden

```
{  
  "error_code" : "APIG.1005",  
  "error_msg" : "No permissions to request this method"  
}
```

Status code: 404

Not Found

```
{  
  "error_code" : "APIG.3004",  
  "error_msg" : "App 9ed8b7fe84224de681e7d7a5587e76dc does not exist"  
}
```

Status code: 500

Internal Server Error

```
{  
  "error_code" : "APIG.9999",  
  "error_msg" : "System error"  
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.29.16 Deleting Access Control Settings of an App

Function

This API is used to delete the access control settings of a credential.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-acl

Table 4-1843 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_id	Yes	String	App ID.

Request Parameters

Table 4-1844 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400**Table 4-1845** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401**Table 4-1846** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-1847** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-1848** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1849** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:app_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3004",
  "error_msg" : "App 9ed8b7fe84224de681e7d7a5587e76dc does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```


Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.30 Credential Quota Management

4.30.1 Creating a Credential Quota

Function

This API is used to create a credential quota.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/app-quotas

Table 4-1850 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1851 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1852 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Quota name. Start with a letter. Use letters, digits, or underscores (_). Minimum: 3 Maximum: 255
call_limits	Yes	Integer	Maximum number of times a credential quota can be called. Minimum: 1 Maximum: 2147483647
time_unit	Yes	String	Time unit. The options are SECOND, MINUTE, HOUR, and DAY.
time_interval	Yes	Integer	Time interval for throttling. Minimum: 1 Maximum: 2147483647
reset_time	No	String	Time when the quota is reset for the first time. If this parameter is not specified, the time is calculated based on the first calling time by default.
remark	No	String	Parameter description. Brackets (<>) are not supported. Maximum: 255

Response Parameters

Status code: 201

Table 4-1853 Response body parameters

Parameter	Type	Description
app_quota_id	String	Credential quota ID.
name	String	Quota name. Enter 3 to 255 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
call_limits	Integer	Maximum number of times a credential quota can be called.
time_unit	String	Time unit. The options are SECOND, MINUTE, HOUR, and DAY.
time_interval	Integer	Time limit of a quota.
remark	String	Parameter description. Maximum: 255
reset_time	String	Time when the quota is reset for the first time. If this parameter is not specified, the time is calculated based on the first calling time by default.
create_time	String	Creation time.
bound_app_num	Integer	Number of applications bound to the quota policy.

Status code: 400

Table 4-1854 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401

Table 4-1855 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-1856** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-1857** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1858** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

```
{
  "call_limits" : 1000,
  "name" : "ClientQuota_demo",
  "reset_time" : "2020-09-20 00:00:00",
  "time_interval" : 1,
  "time_unit" : "DAY"
}
```

Example Responses

Status code: 201

OK

```
{
  "app_quota_id" : "c900c5612dbe451bb43cbcc49cfaf2f3",
  "call_limits" : 1000,
  "create_time" : "2020-09-19T15:27:47.60571141+08:00",
  "name" : "ClientQuota_demo",
  "reset_time" : "2020-09-20 00:00:00",
  "time_interval" : 1,
  "time_unit" : "DAY"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.3325",
  "error_msg" : "The API quota name already exists"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:f0fa1789-3b76-433b-a787-9892951c620ec"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.30.2 Querying Credential Quota Details

Function

This API is used to query credential quota details.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}

Table 4-1859 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_quota_id	Yes	String	Credential Quota ID

Request Parameters

Table 4-1860 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-1861** Response body parameters

Parameter	Type	Description
app_quota_id	String	Credential quota ID.
name	String	Quota name. Enter 3 to 255 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
call_limits	Integer	Maximum number of times a credential quota can be called.
time_unit	String	Time unit. The options are SECOND, MINUTE, HOUR, and DAY.
time_interval	Integer	Time limit of a quota.
remark	String	Parameter description. Maximum: 255
reset_time	String	Time when the quota is reset for the first time. If this parameter is not specified, the time is calculated based on the first calling time by default.
create_time	String	Creation time.
bound_app_num	Integer	Number of applications bound to the quota policy.

Status code: 400

Table 4-1862 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401**Table 4-1863** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-1864** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-1865** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1866** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "app_quota_id" : "c900c5612dbe451bb43cbcc49cfaf2f3",
  "call_limits" : 1000,
  "create_time" : "2020-09-19T07:27:47Z",
  "name" : "ClientQuota_demo",
  "reset_time" : "2020-09-20 00:00:00 +0000 +0000",
  "time_interval" : 1,
  "time_unit" : "DAY"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3093",
  "error_msg" : "App quota c900c5612dbe451bb43cbcc49cfaf2f3 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.30.3 Querying Credential Quotas

Function

This API is used to query credential quotas. Fuzzy query by name is supported.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/app-quotas

Table 4-1867 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1868 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
name	No	String	Credential quota name.

Request Parameters

Table 4-1869 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1870 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.

Parameter	Type	Description
quotas	Array of AppQuotaInfo objects	Credential quotas.

Table 4-1871 AppQuotaInfo

Parameter	Type	Description
app_quota_id	String	Credential quota ID.
name	String	Quota name. Enter 3 to 255 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
call_limits	Integer	Maximum number of times a credential quota can be called.
time_unit	String	Time unit. The options are SECOND, MINUTE, HOUR, and DAY.
time_interval	Integer	Time limit of a quota.
remark	String	Parameter description. Maximum: 255
reset_time	String	Time when the quota is reset for the first time. If this parameter is not specified, the time is calculated based on the first calling time by default.
create_time	String	Creation time.
bound_app_num	Integer	Number of applications bound to the quota policy.

Status code: 400**Table 4-1872** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401

Table 4-1873 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-1874** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1875** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "quotas" : [ {
    "app_quota_id" : "c900c5612dbe451bb43cbcc49cfaf2f3",
    "call_limits" : 1000,
    "create_time" : "2020-09-19T07:27:47Z",
    "name" : "ClientQuota_demo",
    "reset_time" : "2020-09-20 00:00:00 +0000 +0000",
    "time_interval" : 1,
    "time_unit" : "DAY"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:name. Please refer to the support documentation"
}
```

Status code: 401**Unauthorized**

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403**Forbidden**

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500**Internal Server Error**

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.30.4 Modifying a Credential Quota

Function

This API is used to modify a credential quota.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}

Table 4-1876 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_quota_id	Yes	String	Credential Quota ID

Request Parameters

Table 4-1877 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1878 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Quota name. Start with a letter. Use letters, digits, or underscores (_). Minimum: 3 Maximum: 255
call_limits	Yes	Integer	Maximum number of times a credential quota can be called. Minimum: 1 Maximum: 2147483647

Parameter	Mandatory	Type	Description
time_unit	Yes	String	Time unit. The options are SECOND, MINUTE, HOUR, and DAY.
time_interval	Yes	Integer	Time interval for throttling. Minimum: 1 Maximum: 2147483647
reset_time	No	String	Time when the quota is reset for the first time. If this parameter is not specified, the time is calculated based on the first calling time by default.
remark	No	String	Parameter description. Brackets (<>) are not supported. Maximum: 255

Response Parameters

Status code: 200

Table 4-1879 Response body parameters

Parameter	Type	Description
app_quota_id	String	Credential quota ID.
name	String	Quota name. Enter 3 to 255 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
call_limits	Integer	Maximum number of times a credential quota can be called.
time_unit	String	Time unit. The options are SECOND, MINUTE, HOUR, and DAY.
time_interval	Integer	Time limit of a quota.
remark	String	Parameter description. Maximum: 255
reset_time	String	Time when the quota is reset for the first time. If this parameter is not specified, the time is calculated based on the first calling time by default.

Parameter	Type	Description
create_time	String	Creation time.
bound_app_num	Integer	Number of applications bound to the quota policy.

Status code: 400**Table 4-1880** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401**Table 4-1881** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-1882** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-1883** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1884** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

```
{
  "call_limits" : 1000,
  "name" : "ClientQuota_demo",
  "reset_time" : "2020-09-20 00:00:00",
  "time_interval" : 1,
  "time_unit" : "DAY"
}
```

Example Responses**Status code: 200**

OK

```
{
  "app_quota_id" : "c900c5612dbe451bb43cbcc49cfaf2f3",
  "call_limits" : 1000,
  "create_time" : "2020-09-19T07:27:47Z",
  "name" : "ClientQuota_demo",
  "reset_time" : "2020-09-20 00:00:00",
  "time_interval" : 1,
  "time_unit" : "DAY"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.3325",
  "error_msg" : "The API quota name already exists"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3093",
  "error_msg" : "App quota c900c5612dbe451bb43cbcc49cfaf2f3 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.30.5 Deleting a Credential Quota

Function

This API is used to delete a credential quota. When a credential quota is deleted, the association between the quota and credential is also deleted.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}

Table 4-1885 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_quota_id	Yes	String	Credential Quota ID

Request Parameters

Table 4-1886 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

OK

Status code: 400

Table 4-1887 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401

Table 4-1888 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-1889** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-1890** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1891** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2012",
```

```
{
  "error_msg": "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3093",
  "error_msg": "App quota c900c5612dbe451bb43cbcc49cfaf2f3 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
204	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.30.6 Querying the Credentials Bound to a Specified Quota

Function

This API is used to query the credentials bound to a credential quota. Fuzzy match by credential name is supported.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bound-apps

Table 4-1892 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_quota_id	Yes	String	Credential Quota ID

Table 4-1893 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
app_name	No	String	Credential name.

Request Parameters

Table 4-1894 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1895 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
apps	Array of AppQuotaAppInfo objects	Credentials.

Table 4-1896 AppQuotaAppInfo

Parameter	Type	Description
app_id	String	Credential ID.
name	String	Credential name.
status	Integer	Credential status: • 1: enabled • 2: disabled
app_key	String	Credential key.
remark	String	Credential description.
register_time	String	Creation time.
update_time	String	Update time.
app_quota_id	String	Credential quota ID.
app_quota_name	String	Quota name. Enter 3 to 255 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
bound_time	String	Binding time.

Status code: 400**Table 4-1897** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401**Table 4-1898** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403

Table 4-1899 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-1900** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1901** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "apps" : [ {
    "app_id" : "98df09fb-d459-4cbf-83a7-2b55ca6f3d5d",
    "app_key" : "9b93db07-4634-4b7a-99d8-869933ed055d",
    "app_quota_name" : "ClientQuota_demo",
    "bound_time" : "2020-09-19T07:43:11Z",
    "name" : "app-demo",
    "register_time" : "2020-09-18T09:25:19Z",
    "status" : 1,
    "update_time" : "2020-09-18T09:25:19Z"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:app_name. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3093",
  "error_msg" : "The App quota c900c5612dbe451bb43bcc49cfaf2f3 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.30.7 Binding a Credential Quota with Credentials

Function

This API is used to bind a credential quota with credentials.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/binding-apps

Table 4-1902 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_quota_id	Yes	String	Credential Quota ID

Request Parameters

Table 4-1903 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1904 Request body parameters

Parameter	Mandatory	Type	Description
app_ids	Yes	Array of strings	Credential ID List.

Response Parameters

Status code: 201

Table 4-1905 Response body parameters

Parameter	Type	Description
applies	Array of AppQuotaAppBinding objects	Credential and credential quota binding list.

Table 4-1906 AppQuotaAppBinding

Parameter	Type	Description
app_quota_id	String	Credential quota ID.
app_id	String	Credential ID.
bound_time	String	Binding time.

Status code: 400

Table 4-1907 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401

Table 4-1908 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error description.

Status code: 403**Table 4-1909** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-1910** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1911** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

```
{
  "app_ids" : [ "98df09fb-d459-4cbf-83a7-2b55ca6f3d5d" ]
}
```

Example Responses

Status code: 201

OK

```
{
  "applies" : [ {
    "app_id" : "98df09fb-d459-4cbf-83a7-2b55ca6f3d5d",
```

```
{
  "app_quota_id" : "c900c5612dbe451bb43cbcc49cfaf2f3",
  "bound_time" : "2020-09-19T07:43:11.948178051Z"
}]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3093",
  "error_msg" : "The App quota c900c5612dbe451bb43cbcc49cfaf2f3 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

Status Code	Description
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.30.8 Unbinding a Credential Quota from a Credential

Function

This API is used to unbind a credential quota from a credential.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bound-apps/{app_id}

Table 4-1912 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_quota_id	Yes	String	Credential Quota ID
app_id	Yes	String	App ID.

Request Parameters

Table 4-1913 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

OK

Status code: 400

Table 4-1914 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401

Table 4-1915 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403

Table 4-1916 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-1917** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1918** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support
documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3093",
  "error_msg" : "The App quota c900c5612dbe451bb43bcc49cfaf2f3 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
204	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.30.9 Querying Credentials That Can Be Bound to a Credential Quota

Function

This API is used to query the credentials that can be bound to a credential quota. Fuzzy search by credential name is supported.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bindable-apps

Table 4-1919 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
app_quota_id	Yes	String	Credential Quota ID

Table 4-1920 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
app_name	No	String	App name.

Request Parameters

Table 4-1921 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1922 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
apps	Array of AppQuotaAppInfo objects	Credentials.

Table 4-1923 AppQuotaAppInfo

Parameter	Type	Description
app_id	String	Credential ID.
name	String	Credential name.
status	Integer	Credential status: 1: enabled 2: disabled
app_key	String	Credential key.
remark	String	Credential description.
register_time	String	Creation time.
update_time	String	Update time.
app_quota_id	String	Credential quota ID.
app_quota_name	String	Quota name. Enter 3 to 255 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
bound_time	String	Binding time.

Status code: 400

Table 4-1924 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401**Table 4-1925** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-1926** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-1927** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1928** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "apps" : [ {
    "app_id" : "ac18a23f-8f06-40ac-8093-f790de2ba95b",
    "app_key" : "ac18a23f-8f06-40ac-8093-f790de2ba95b",
    "bound_time" : "0001-01-01T00:00:00Z",
    "name" : "app-test",
    "register_time" : "2020-08-22T07:57:01Z",
    "status" : 1,
    "update_time" : "2020-08-22T07:57:01Z"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3093",
  "error_msg" : "The App quota c900c5612dbe451bb43bcc49cfaf2f3 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
}
```

```
"error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.31 Asynchronous Task Management

4.31.1 Exporting APIs Asynchronously

Function

This API is used to export APIs in a specified API group. The content of the exported file complies with the Swagger standard. For details about the custom extended fields of APIG, see section "Importing and Exporting APIs" > "Extended Definition" in the API Gateway User Guide.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/openapi/async-export

Table 4-1929 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1930 Query Parameters

Parameter	Mandatory	Type	Description
oas_version	No	String	OpenAPI version. Default: 2.0

Request Parameters

Table 4-1931 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1932 Request body parameters

Parameter	Mandatory	Type	Description
env_id	Yes	String	ID of the environment in which APIs of a group have been published.
group_id	Yes	String	API group ID.

Parameter	Mandatory	Type	Description
define	No	String	Definition scope of the APIs to be exported: • spec: basic definitions, including only the frontend definitions. • proxy: full definitions, including the frontend and backend definitions. • all: extended definitions, including the frontend and backend definitions as well as request throttling policies, access control policies, and custom authorizers. • dev: development definitions, including the frontend and backend definitions of APIs that have not been published. Default: spec
type	No	String	Format for exporting API definitions. Default: json
version	No	String	Version number of the APIs after exporting. The default value is the current date and time.
apis	No	Array of strings	IDs of the APIs to be exported.

Response Parameters

Status code: 202

Table 4-1933 Response body parameters

Parameter	Type	Description
task_id	String	Task ID.

Status code: 400

Table 4-1934 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1935** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1936** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1937** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Exporting APIs in batches

```
{
  "env_id" : "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "group_id" : "c77f5e81d9cb4424bf704ef2b0ac7600",
  "define" : "all"
}
```

Example Responses

Status code: 202

Accepted

```
{
  "task_id" : "d9ce8c9eede54b3f841ec324fe0bfdc2"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2001",
  "error_msg" : "The request parameters must be specified,parameterName:env_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
202	Accepted
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.31.2 Importing APIs Asynchronously

Function

This API is used to import APIs. The content of the imported file must comply with the Swagger standard. For details about the custom extended fields of APIG, see section "Importing and Exporting APIs" > "Extended Definition" in the API Gateway User Guide.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/openapi/async-import

Table 4-1938 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1939 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1940 FormData parameters

Parameter	Mandatory	Type	Description
is_create_group	No	Boolean	Whether to create a new group. Default: true
group_id	No	String	API group ID. This parameter is required if is_create_group is set to false.
extend_mode	No	String	Import mode of extended information. • merge: Retain the original extended information if a conflict occurs. • override: Override the original extended information if a conflict occurs. Default: merge
simple_mode	No	Boolean	Whether to enable fast import. Default: false
mock_mode	No	Boolean	Whether to enable the Mock backend. Default: false
api_mode	No	String	Import mode. • merge: Retain the original API information if a conflict occurs. • override: Override the original API information if a conflict occurs. Default: merge
file_name	Yes	File	Request body in JSON or YAML format for importing APIs

Response Parameters

Status code: 202

Table 4-1941 Response body parameters

Parameter	Type	Description
task_id	String	Task ID.

Status code: 400**Table 4-1942** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1943** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1944** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1945** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Importing APIs

```
{
  "is_create_group" : false,
  "group_id" : "d9ce8c9eede54b3f841ec324fe0bfdc2",
  "file_name" : "APIGroup_test.json"
}
```

Example Responses

Status code: 202

Accepted

```
{
  "task_id" : "d9ce8c9eede54b3f841ec324fe0bfdc2"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.3603",
  "error_msg" : "The input data is too long"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
202	Accepted
400	Bad Request

Status Code	Description
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.31.3 Querying the Result of an Asynchronous Task

Function

This API is used to query the result of an asynchronous task.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/async-tasks/{task_id}

Table 4-1946 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
task_id	Yes	String	Asynchronous task ID.

Request Parameters

Table 4-1947 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-1948** Response body parameters

Parameter	Type	Description
task_id	String	Task ID.
task_status	String	Task status. Options: waiting, processing, succeed, and failed.
task_type	String	Task type. Options: import_api and export_api. Both types of tasks are asynchronous.
task_result	String	Task result. A string can be converted into a JSON object. If task_type is set to import_api, the fields include group_id, success (array), failure (array), swagger (structure), and ignore (array). The success array contains four fields: id (ID of a successfully imported API), method (API request method), path (API request path), and action (update or create). The failure array also contains four fields: method (API request method), path (API request path), error_code (import error code), and error_msg (import error message). The swagger structure contains two fields: id (Swagger file ID) and result (import result). The ignore array has two elements: method (API request method) and path (API request path). If task_type is set to export_api, the fields include file_type and content.

Status code: 400**Table 4-1949** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-1950** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-1951** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-1952** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-1953** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

- Example 1

```
{
  "task_id" : "d9ce8c9eede54b3f841ec324fe0bfcdc2",
  "task_status" : "succeed",
  "task_type" : "import_api",
  "task_result" : "{ \"success\": [{ \"id\": \"ee93ce6815f04896b301452982b92222\", \"action\": \"create\", \"method\": \"GET\", \"path\": \"/test1\" }], \"failure\": [], \"swagger\": { \"id\": \"de1852ab6c5e4090b0bd88a02058e650\", \"result\": \"Success\" }, \"group_id\": \"9100ae30705947cc9543d37cd7fb388c\" }"
```

- Example 2

```
{
  "task_id" : "d6e8834b6f0f4711a2fa5345e5b60833",
  "task_status" : "succeed",
  "task_type" : "export_api",
  "task_result" : "{ \"FileName\": \"test8-RELEASE-all-2023-07-11-19:54:22\", \"FileType\": \"json\", \"Comment\": \"\", \"swagger\": { \"2.0\": { \"info\": { \"title\": \"test8\", \"version\": \"2023-07-11-19:54:22\", \"host\": \"9100ae30705947cc9543d37cd7fb388c.apic.example.com\", \"paths\": { \"test1\": { \"get\": { \"security\": [ \"apig-auth-app\" ], \"schemes\": [ \"https\" ], \"operationId\": \"API_zjev\", \"responses\": { \"default\": { \"x-apigateway-result-failure-sample\": \"\", \"x-apigateway-result-normal-sample\": \"\", \"x-apigateway-backend\": { \"mockEndpoints\": { \"description\": \"\", \"result-content\": \"not ok\", \"type\": \"MOCK\" }, \"x-apigateway-cors\": false, \"x-apigateway-match-mode\": \"NORMAL\", \"x-apigateway-request-type\": \"public\", \"responses\": { \"default\": { \"description\": \"response example\" }, \"securityDefinitions\": { \"apig-auth-app\": { \"apiKey\": \"\", \"name\": \"Authorization\", \"in\": \"header\", \"x-apigateway-auth-opt\": { \"appcode-auth-type\": \"\", \"x-apigateway-auth-type\": \"AppSigv1\", \"apig-auth-iam\": { \"apiKey\": \"\", \"name\": \"\", \"unused\": \"\", \"x-apigateway-auth-type\": \"IAM\" } } } } } } } } }
```

- Example 3

```
{
  "task_id" : "f01d2772ea4944408fa544c8ae5a9999",
  "task_status" : "failed",
  "task_type" : "import_api",
  "task_result" : "{ \"error_code\": \"APIG.3201\", \"error_msg\": \"The API group name already exists\" }
```

- Example 4

```
{
  "task_id" : "4dfbf6acaacf4c41a8b3c50daa90d3dc",
  "task_status" : "processing",
  "task_type" : "import_api",
  "task_result" : ""
}
```

- Example 5

```
{
  "task_id" : "c3b78a52fb28461aab92bf6c6989f731",
  "task_status" : "waiting",
  "task_type" : "import_api",
  "task_result" : ""
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2001",
  "error_msg" : "The request parameters must be specified,parameterName:task_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3093",
  "error_msg" : "The asynchronous task d9ce8c9eede54b3f841ec324fe0bfdc2 does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.32 Orchestration Rule Management

4.32.1 Creating an Orchestration Rule

Function

This API is used to create an orchestration rule.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/orchestrations

Table 4-1954 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-1955 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1956 Request body parameters

Parameter	Mandatory	Type	Description
orchestration_name	Yes	String	Orchestration mapping rule name. The name must be 3 to 64 characters long, start with a letter and use only letters, digits, and underscores (_). It must be unique in the same gateway. Minimum: 3 Maximum: 64
orchestration_strategy	Yes	String	Orchestration policy. Options: • list • hash • range • hash_range • none_value • default • head_n • tail_n. If the orchestration policy is list, the number of objects in orchestration_map multiplied by that in map_param_list cannot exceed 3,000.
orchestration_mapped_param	No	OrchestrationMappedParam object	Parameter configuration after orchestration. This parameter is mandatory when isPreprocessing is set to false.

Parameter	Mandatory	Type	Description
is_preprocessing	No	Boolean	Indicates whether the policy is a preprocessing policy. A preprocessing policy generates only temporary parameters as the input of the subsequent parameter orchestration rule. And it cannot be used as the last orchestration rule except the default orchestration rule.
orchestration_map	No	Array of OrchestrationMap objects	List of orchestration mapping rules. The list contains 1 to 300 characters. Orchestration mapping rules are prioritized in the same sequence as the the list. Mapping rules must be unique. If orchestration_strategy is list, map_param_list cannot contain same elements. Array Length: 1 - 300

Table 4-1957 OrchestrationMappedParam

Parameter	Mandatory	Type	Description
mapped_param_name	Yes	String	Name of the request parameter after orchestration. The value can contain 1 to 128 characters, including letters, digits, and hyphens (-). It must start with a letter and cannot be the same as an existing parameter name. By default, the parameter name is transparently transmitted to the backend. Minimum: 1 Maximum: 128
mapped_param_type	Yes	String	Type of the parameter after orchestration. The value can be string or number.
mapped_param_location	Yes	String	Position of the orchestrated parameter. The value can be query or header.

Table 4-1958 OrchestrationMap

Parameter	Mandatory	Type	Description
map_param_list	No	Array of strings	List of parameters after mapping orchestration. This parameter is mandatory when orchestration_strategy is set to list. The list length ranges from 0 to 3000. The value can contain 1 to 128 characters, including letters, digits, hyphens (-), and underscores (_). Minimum: 1 Maximum: 128 Array Length: 0 - 3000
map_param_range	No	OrchestrationMapParamRange object	This parameter is for mapping range configurations of parameters after orchestration and is mandatory if orchestration_strategy is range or hash_range.
mapped_param_value	No	String	The parameter value after orchestration can contain 1 to 128 characters, including only letters and digits. This parameter is optional only when orchestration_strategy is set to hash, head_n, or tail_n, or is_preprocessing is set to false. Minimum: 0 Maximum: 128
intercept_length	No	Integer	Truncation length. The value ranges from 1 to 100. This parameter is mandatory when the policy type is head_n or tail_n. If the truncation length is greater than the parameter length, the parameter truncation result is a complete parameter. Minimum: 1 Maximum: 100

Table 4-1959 OrchestrationMapParamRange

Parameter	Mandatory	Type	Description
range_start	No	String	Range start value. The value is a string that can be converted to an integer. After the conversion, the value of range_start ranges from 0 to 9223372036854775807. And the value of range_start cannot be greater than that of range_end.
range_end	No	String	Range end value. The value is a string that can be converted to an integer. After the conversion, the value of range_end ranges from 0 to 9223372036854775807. And the value of range_start cannot be greater than that of range_end.

Response Parameters

Status code: 201

Table 4-1960 Response body parameters

Parameter	Type	Description
orchestration_name	String	Orchestration mapping rule name. The name must be 3 to 64 characters long, start with a letter and use only letters, digits, and underscores (_). It must be unique in the same gateway. Minimum: 3 Maximum: 64

Parameter	Type	Description
orchestration_strategy	String	Orchestration policy. Options: • list • hash • range • hash_range • none_value • default • head_n • tail_n. If the orchestration policy is list, the number of objects in orchestration_map multiplied by that in map_param_list cannot exceed 3,000.
orchestration_mapped_param	OrchestrationMappedParam object	Parameter configuration after orchestration. This parameter is mandatory when isPreprocessing is set to false.
is_preprocessing	Boolean	Indicates whether the policy is a preprocessing policy. A preprocessing policy generates only temporary parameters as the input of the subsequent parameter orchestration rule. And it cannot be used as the last orchestration rule except the default orchestration rule.
orchestration_map	Array of OrchestrationMap objects	List of orchestration mapping rules. The list contains 1 to 300 characters. Orchestration mapping rules are prioritized in the same sequence as the the list. Mapping rules must be unique. If orchestration_strategy is list, map_param_list cannot contain same elements. Array Length: 1 - 300
orchestration_id	String	Orchestration rule ID.
orchestration_create_time	String	Time when an orchestration rule was created.
orchestration_update_time	String	Time when an orchestration rule was updated.

Table 4-1961 OrchestrationMappedParam

Parameter	Type	Description
mapped_param_name	String	Name of the request parameter after orchestration. The value can contain 1 to 128 characters, including letters, digits, and hyphens (-). It must start with a letter and cannot be the same as an existing parameter name. By default, the parameter name is transparently transmitted to the backend. Minimum: 1 Maximum: 128
mapped_param_type	String	Type of the parameter after orchestration. The value can be string or number.
mapped_param_location	String	Position of the orchestrated parameter. The value can be query or header.

Table 4-1962 OrchestrationMap

Parameter	Type	Description
map_param_list	Array of strings	List of parameters after mapping orchestration. This parameter is mandatory when orchestration_strategy is set to list. The list length ranges from 0 to 3000. The value can contain 1 to 128 characters, including letters, digits, hyphens (-), and underscores (_). Minimum: 1 Maximum: 128 Array Length: 0 - 3000
map_param_range	OrchestrationMapParamRange object	This parameter is for mapping range configurations of parameters after orchestration and is mandatory if orchestration_strategy is range or hash_range.

Parameter	Type	Description
mapped_param_value	String	The parameter value after orchestration can contain 1 to 128 characters, including only letters and digits. This parameter is optional only when orchestration_strategy is set to hash, head_n, or tail_n, or is_preprocessing is set to false. Minimum: 0 Maximum: 128
intercept_length	Integer	Truncation length. The value ranges from 1 to 100. This parameter is mandatory when the policy type is head_n or tail_n. If the truncation length is greater than the parameter length, the parameter truncation result is a complete parameter. Minimum: 1 Maximum: 100

Table 4-1963 OrchestrationMapParamRange

Parameter	Type	Description
range_start	String	Range start value. The value is a string that can be converted to an integer. After the conversion, the value of range_start ranges from 0 to 9223372036854775807. And the value of range_start cannot be greater than that of range_end.
range_end	String	Range end value. The value is a string that can be converted to an integer. After the conversion, the value of range_end ranges from 0 to 9223372036854775807. And the value of range_start cannot be greater than that of range_end.

Status code: 400

Table 4-1964 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401**Table 4-1965** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-1966** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-1967** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1968** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

- Creating a **list** orchestration rule

```
{
  "orchestration_name": "orchestration_demo_1",
  "orchestration_strategy": "list",
  "orchestration_mapped_param": {
    "mapped_param_name": "shared-tag",
    "mapped_param_type": "number",
    "mapped_param_location": "header"
  },
  "orchestration_map": [ {
    "map_param_list": [ "10001", "10002" ],
    "mapped_param_value": "1"
  }, {
    "map_param_list": [ "10003", "10004" ],
    "mapped_param_value": "2"
  } ],
  "is_preprocessing": false
}
```

- Creating a **range** orchestration rule

```
{
  "orchestration_name": "orchestration_demo_2",
  "orchestration_strategy": "range",
  "orchestration_mapped_param": {
    "mapped_param_name": "shared-tag",
    "mapped_param_type": "number",
    "mapped_param_location": "header"
  },
  "orchestration_map": [ {
    "map_param_range": {
      "range_start": "1",
      "range_end": "1000"
    },
    "mapped_param_value": "1"
  } ]
}
```

- Creating a **hash** orchestration rule

```
{
  "orchestration_name": "orchestration_demo_3",
  "orchestration_strategy": "hash",
  "orchestration_mapped_param": {
    "mapped_param_name": "shared-tag",
    "mapped_param_type": "number",
    "mapped_param_location": "header"
  }
}
```

- Creating a **hash_range** orchestration rule

```
{
  "orchestration_name": "orchestration_demo_4",
  "orchestration_strategy": "hash_range",
  "orchestration_mapped_param": {
    "mapped_param_name": "shared-tag",
    "mapped_param_type": "number",
    "mapped_param_location": "header"
  },
  "orchestration_map": [ {
    "map_param_range": {
      "range_start": "1",
      "range_end": "1000"
    },
    "mapped_param_value": "1"
  } ]
}
```

- Creating a **none_value** orchestration rule

```
{
  "orchestration_name": "orchestration_demo_5",
  "orchestration_strategy": "none_value",
  "orchestration_mapped_param": {
    "mapped_param_name": "shared-tag",
    "mapped_param_type": "number",
    "mapped_param_location": "header"
  },
  "orchestration_map": [ {
    "mapped_param_value": "1"
  } ]
}
```

- Creating a **default** orchestration rule

```
{
  "orchestration_name": "orchestration_demo_6",
  "orchestration_strategy": "default",
  "orchestration_mapped_param": {
    "mapped_param_name": "shared-tag",
    "mapped_param_type": "number",
    "mapped_param_location": "header"
  },
  "orchestration_map": [ {
    "mapped_param_value": "1"
  } ]
}
```

- Creating a **head_n** orchestration rule

```
{
  "orchestration_name": "orchestration_demo_7",
  "orchestration_strategy": "head_n",
  "orchestration_mapped_param": {
    "mapped_param_name": "shared-tag",
    "mapped_param_type": "number",
    "mapped_param_location": "header"
  },
  "orchestration_map": [ {
    "intercept_length": 10,
    "mapped_param_value": "1"
  } ]
}
```

- Creating a **tail_n** orchestration rule

```
{
  "orchestration_name": "orchestration_demo_8",
  "orchestration_strategy": "tail_n",
  "orchestration_mapped_param": {
    "mapped_param_name": "shared-tag",
    "mapped_param_type": "number",
    "mapped_param_location": "header"
  },
  "orchestration_map": [ {
    "intercept_length": 10,
    "mapped_param_value": "1"
  } ]
}
```

- Creating a **tail_n** preprocessing orchestration rule

```
{
  "orchestration_name": "orchestration_demo_8",
  "orchestration_strategy": "tail_n",
  "orchestration_mapped_param": {
    "mapped_param_name": "shared-tag",
    "mapped_param_type": "number",
    "mapped_param_location": "header"
  },
  "orchestration_map": [ {
    "intercept_length": 10
  } ],
}
```



```
"is_preprocessing" : true
}
```

Example Responses

Status code: 201

Created

- Example 1

```
{
  "orchestration_id" : "76545e81d9cb4424bf704ef2b0ac7600",
  "orchestration_name" : "orchestration_demo_1",
  "orchestration_create_time" : "2023-07-02T12:31:23.353Z",
  "orchestration_update_time" : "2023-07-02T13:31:23.353Z",
  "orchestration_strategy" : "list",
  "orchestration_mapped_param" : {
    "mapped_param_name" : "shared-tag",
    "mapped_param_type" : "number",
    "mapped_param_location" : "header"
  },
  "orchestration_map" : [ {
    "map_param_list" : [ "10001", "10002" ],
    "mapped_param_value" : "1"
  }, {
    "map_param_list" : [ "10003", "10004" ],
    "mapped_param_value" : "2"
  } ]
}
```

- Example 2

```
{
  "orchestration_id" : "yt655e81d9cb4424bf704ef2b0ac7600",
  "orchestration_name" : "orchestration_demo_2",
  "orchestration_create_time" : "2023-07-02T12:31:23.353Z",
  "orchestration_update_time" : "2023-07-02T13:31:23.353Z",
  "orchestration_strategy" : "range",
  "orchestration_mapped_param" : {
    "mapped_param_name" : "shared-tag",
    "mapped_param_type" : "number",
    "mapped_param_location" : "header"
  },
  "orchestration_map" : [ {
    "map_param_range" : {
      "range_start" : "1",
      "range_end" : "1000"
    },
    "mapped_param_value" : "1"
  } ]
}
```

- Example 3

```
{
  "orchestration_id" : "a7655e81d9cb4424bf704ef2b0ac7600",
  "orchestration_name" : "orchestration_demo_3",
  "orchestration_create_time" : "2023-07-02T12:31:23.353Z",
  "orchestration_update_time" : "2023-07-02T13:31:23.353Z",
  "orchestration_strategy" : "hash",
  "orchestration_mapped_param" : {
    "mapped_param_name" : "shared-tag",
    "mapped_param_type" : "number",
    "mapped_param_location" : "header"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:f0fa1789-3b76-433b-a787-9892951c620ec"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.32.2 Viewing Orchestration Rules

Function

This API is used to view orchestration rules.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/orchestrations

Table 4-1969 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-1970 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
orchestration_name	No	String	Orchestration rule name.

Parameter	Mandatory	Type	Description
precise_search	No	String	Parameter name for exact matching. Separate multiple parameter names with commas (,). Only orchestration_name is supported.
orchestration_id	No	String	Orchestration rule ID. Separate multiple orchestration rule IDs with commas (,). The maximum number of IDs is the maximum number of rules that can be bound to an API. For details, see "Quotas" in APIG Service Overview.

Request Parameters

Table 4-1971 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1972 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
orchestrations	Array of OrchestrationBaseResp objects	Orchestration rules that are queried.

Table 4-1973 OrchestrationBaseResp

Parameter	Type	Description
orchestration_name	String	Orchestration mapping rule name. The name must be 3 to 64 characters long, start with a letter and use only letters, digits, and underscores (_). It must be unique in the same gateway. Minimum: 3 Maximum: 64
orchestration_strategy	String	Orchestration policy. Options: • list • hash • range • hash_range • none_value • default • head_n • tail_n. If the orchestration policy is list, the number of objects in orchestration_map multiplied by that in map_param_list cannot exceed 3,000.
orchestration_mapped_param	OrchestrationMappedParam object	Parameter configuration after orchestration. This parameter is mandatory when isPreprocessing is set to false.
is_preprocessing	Boolean	Indicates whether the policy is a preprocessing policy. A preprocessing policy generates only temporary parameters as the input of the subsequent parameter orchestration rule. And it cannot be used as the last orchestration rule except the default orchestration rule.
orchestration_id	String	Orchestration rule ID.
orchestration_create_time	String	Time when an orchestration rule was created.
orchestration_update_time	String	Time when an orchestration rule was updated.

Table 4-1974 OrchestrationMappedParam

Parameter	Type	Description
mapped_param_name	String	Name of the request parameter after orchestration. The value can contain 1 to 128 characters, including letters, digits, and hyphens (-). It must start with a letter and cannot be the same as an existing parameter name. By default, the parameter name is transparently transmitted to the backend. Minimum: 1 Maximum: 128
mapped_param_type	String	Type of the parameter after orchestration. The value can be string or number.
mapped_param_location	String	Position of the orchestrated parameter. The value can be query or header.

Status code: 400**Table 4-1975** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401**Table 4-1976** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403

Table 4-1977 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404

Table 4-1978 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500

Table 4-1979 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total": 2,
  "size": 2,
  "orchestrations": [ {
    "orchestration_id": "76545e81d9cb4424bf704ef2b0ac7600",
    "orchestration_name": "orchestration_demo_1",
    "orchestration_create_time": "2023-07-02T12:31:23.353Z",
    "orchestration_update_time": "2023-07-02T13:31:23.353Z",
    "orchestration_strategy": "list",
    "orchestration_mapped_param": {
      "mapped_param_name": "shared-tag",
      "mapped_param_type": "number",
      "mapped_param_location": "header"
    }
  }, {
    "orchestration_id": "yt655e81d9cb4424bf704ef2b0ac7600",
```

```
"orchestration_name" : "orchestration_demo_2",
"orchestration_create_time" : "2023-07-02T12:31:23.353Z",
"orchestration_update_time" : "2023-07-02T13:31:23.353Z",
"orchestration_strategy" : "range",
"orchestration_mapped_param" : {
  "mapped_param_name" : "shared-tag",
  "mapped_param_type" : "number",
  "mapped_param_location" : "header"
}
}]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:f0fa1789-3b76-433b-a787-9892951c620ec"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request

Status Code	Description
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.32.3 Querying Rule Details

Function

This API is used to query orchestration rule details.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/orchestrations/{orchestration_id}

Table 4-1980 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
orchestration_id	Yes	String	Orchestration rule ID.

Request Parameters

Table 4-1981 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-1982** Response body parameters

Parameter	Type	Description
orchestration_name	String	Orchestration mapping rule name. The name must be 3 to 64 characters long, start with a letter and use only letters, digits, and underscores (_). It must be unique in the same gateway. Minimum: 3 Maximum: 64
orchestration_strategy	String	Orchestration policy. Options: • list • hash • range • hash_range • none_value • default • head_n • tail_n. If the orchestration policy is list, the number of objects in orchestration_map multiplied by that in map_param_list cannot exceed 3,000.
orchestration_mapped_param	OrchestrationMappedParam object	Parameter configuration after orchestration. This parameter is mandatory when isPreprocessing is set to false.

Parameter	Type	Description
is_preprocessing	Boolean	Indicates whether the policy is a preprocessing policy. A preprocessing policy generates only temporary parameters as the input of the subsequent parameter orchestration rule. And it cannot be used as the last orchestration rule except the default orchestration rule.
orchestration_map	Array of OrchestrationMap objects	List of orchestration mapping rules. The list contains 1 to 300 characters. Orchestration mapping rules are prioritized in the same sequence as the the list. Mapping rules must be unique. If orchestration_strategy is list, map_param_list cannot contain same elements. Array Length: 1 - 300
orchestration_id	String	Orchestration rule ID.
orchestration_create_time	String	Time when an orchestration rule was created.
orchestration_update_time	String	Time when an orchestration rule was updated.

Table 4-1983 OrchestrationMappedParam

Parameter	Type	Description
mapped_param_name	String	Name of the request parameter after orchestration. The value can contain 1 to 128 characters, including letters, digits, and hyphens (-). It must start with a letter and cannot be the same as an existing parameter name. By default, the parameter name is transparently transmitted to the backend. Minimum: 1 Maximum: 128
mapped_param_type	String	Type of the parameter after orchestration. The value can be string or number.

Parameter	Type	Description
mapped_param_location	String	Position of the orchestrated parameter. The value can be query or header.

Table 4-1984 OrchestrationMap

Parameter	Type	Description
map_param_list	Array of strings	List of parameters after mapping orchestration. This parameter is mandatory when orchestration_strategy is set to list. The list length ranges from 0 to 3000. The value can contain 1 to 128 characters, including letters, digits, hyphens (-), and underscores (_). Minimum: 1 Maximum: 128 Array Length: 0 - 3000
map_param_range	OrchestrationMapParamRange object	This parameter is for mapping range configurations of parameters after orchestration and is mandatory if orchestration_strategy is range or hash_range.
mapped_param_value	String	The parameter value after orchestration can contain 1 to 128 characters, including only letters and digits. This parameter is optional only when orchestration_strategy is set to hash, head_n, or tail_n, or is_preprocessing is set to false. Minimum: 0 Maximum: 128
intercept_length	Integer	Truncation length. The value ranges from 1 to 100. This parameter is mandatory when the policy type is head_n or tail_n. If the truncation length is greater than the parameter length, the parameter truncation result is a complete parameter. Minimum: 1 Maximum: 100

Table 4-1985 OrchestrationMapParamRange

Parameter	Type	Description
range_start	String	Range start value. The value is a string that can be converted to an integer. After the conversion, the value of range_start ranges from 0 to 9223372036854775807. And the value of range_start cannot be greater than that of range_end.
range_end	String	Range end value. The value is a string that can be converted to an integer. After the conversion, the value of range_end ranges from 0 to 9223372036854775807. And the value of range_start cannot be greater than that of range_end.

Status code: 400**Table 4-1986** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401**Table 4-1987** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-1988** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-1989** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-1990** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

Example Responses**Status code: 200**

OK

```
{
  "orchestration_id" : "yt655e81d9cb4424bf704ef2b0ac7600",
  "orchestration_name" : "orchestration_demo_1",
  "orchestration_create_time" : "2023-07-02T12:31:23.353Z",
  "orchestration_update_time" : "2023-07-02T13:31:23.353Z",
  "orchestration_strategy" : "range",
  "orchestration_mapped_param" : {
    "mapped_param_name" : "shared-tag",
    "mapped_param_type" : "number",
    "mapped_param_location" : "header"
  },
  "orchestration_map" : [ {
    "map_param_range" : {
      "range_start" : "1",
      "range_end" : "1000"
    },
    "mapped_param_value" : "1"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:domain_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3020",
  "error_msg" : "The URL domain does not exist"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.32.4 Updating an Orchestration Rule

Function

This API is used to update an orchestration rule.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v2/{project_id}/apigw/instances/{instance_id}/orchestrations/{orchestration_id}

Table 4-1991 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
orchestration_id	Yes	String	Orchestration rule ID.

Request Parameters

Table 4-1992 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1993 Request body parameters

Parameter	Mandatory	Type	Description
orchestration_name	Yes	String	Orchestration mapping rule name. The name must be 3 to 64 characters long, start with a letter and use only letters, digits, and underscores (_). It must be unique in the same gateway. Minimum: 3 Maximum: 64
orchestration_strategy	Yes	String	Orchestration policy. Options: • list • hash • range • hash_range • none_value • default • head_n • tail_n. If the orchestration policy is list, the number of objects in orchestration_map multiplied by that in map_param_list cannot exceed 3,000.
orchestration_mapped_param	No	OrchestrationMappedParam object	Parameter configuration after orchestration. This parameter is mandatory when isPreprocessing is set to false.
is_preprocessing	No	Boolean	Indicates whether the policy is a preprocessing policy. A preprocessing policy generates only temporary parameters as the input of the subsequent parameter orchestration rule. And it cannot be used as the last orchestration rule except the default orchestration rule.

Parameter	Mandatory	Type	Description
orchestration_map	No	Array of OrchestrationMap objects	List of orchestration mapping rules. The list contains 1 to 300 characters. Orchestration mapping rules are prioritized in the same sequence as the the list. Mapping rules must be unique. If orchestration_strategy is list, map_param_list cannot contain same elements. Array Length: 1 - 300

Table 4-1994 OrchestrationMappedParam

Parameter	Mandatory	Type	Description
mapped_param_name	Yes	String	Name of the request parameter after orchestration. The value can contain 1 to 128 characters, including letters, digits, and hyphens (-). It must start with a letter and cannot be the same as an existing parameter name. By default, the parameter name is transparently transmitted to the backend. Minimum: 1 Maximum: 128
mapped_param_type	Yes	String	Type of the parameter after orchestration. The value can be string or number.
mapped_param_location	Yes	String	Position of the orchestrated parameter. The value can be query or header.

Table 4-1995 OrchestrationMap

Parameter	Mandatory	Type	Description
map_param_list	No	Array of strings	List of parameters after mapping orchestration. This parameter is mandatory when orchestration_strategy is set to list. The list length ranges from 0 to 3000. The value can contain 1 to 128 characters, including letters, digits, hyphens (-), and underscores (_). Minimum: 1 Maximum: 128 Array Length: 0 - 3000
map_param_range	No	OrchestrationMapParamRange object	This parameter is for mapping range configurations of parameters after orchestration and is mandatory if orchestration_strategy is range or hash_range.
mapped_param_value	No	String	The parameter value after orchestration can contain 1 to 128 characters, including only letters and digits. This parameter is optional only when orchestration_strategy is set to hash, head_n, or tail_n, or is_preprocessing is set to false. Minimum: 0 Maximum: 128
intercept_length	No	Integer	Truncation length. The value ranges from 1 to 100. This parameter is mandatory when the policy type is head_n or tail_n. If the truncation length is greater than the parameter length, the parameter truncation result is a complete parameter. Minimum: 1 Maximum: 100

Table 4-1996 OrchestrationMapParamRange

Parameter	Mandatory	Type	Description
range_start	No	String	Range start value. The value is a string that can be converted to an integer. After the conversion, the value of range_start ranges from 0 to 9223372036854775807. And the value of range_start cannot be greater than that of range_end.
range_end	No	String	Range end value. The value is a string that can be converted to an integer. After the conversion, the value of range_end ranges from 0 to 9223372036854775807. And the value of range_start cannot be greater than that of range_end.

Response Parameters

Status code: 200

Table 4-1997 Response body parameters

Parameter	Type	Description
orchestration_name	String	Orchestration mapping rule name. The name must be 3 to 64 characters long, start with a letter and use only letters, digits, and underscores (_). It must be unique in the same gateway. Minimum: 3 Maximum: 64

Parameter	Type	Description
orchestration_strategy	String	Orchestration policy. Options: • list • hash • range • hash_range • none_value • default • head_n • tail_n. If the orchestration policy is list, the number of objects in orchestration_map multiplied by that in map_param_list cannot exceed 3,000.
orchestration_mapped_param	OrchestrationMappedParam object	Parameter configuration after orchestration. This parameter is mandatory when isPreprocessing is set to false.
is_preprocessing	Boolean	Indicates whether the policy is a preprocessing policy. A preprocessing policy generates only temporary parameters as the input of the subsequent parameter orchestration rule. And it cannot be used as the last orchestration rule except the default orchestration rule.
orchestration_map	Array of OrchestrationMap objects	List of orchestration mapping rules. The list contains 1 to 300 characters. Orchestration mapping rules are prioritized in the same sequence as the the list. Mapping rules must be unique. If orchestration_strategy is list, map_param_list cannot contain same elements. Array Length: 1 - 300
orchestration_id	String	Orchestration rule ID.
orchestration_create_time	String	Time when an orchestration rule was created.
orchestration_update_time	String	Time when an orchestration rule was updated.

Table 4-1998 OrchestrationMappedParam

Parameter	Type	Description
mapped_param_name	String	Name of the request parameter after orchestration. The value can contain 1 to 128 characters, including letters, digits, and hyphens (-). It must start with a letter and cannot be the same as an existing parameter name. By default, the parameter name is transparently transmitted to the backend. Minimum: 1 Maximum: 128
mapped_param_type	String	Type of the parameter after orchestration. The value can be string or number.
mapped_param_location	String	Position of the orchestrated parameter. The value can be query or header.

Table 4-1999 OrchestrationMap

Parameter	Type	Description
map_param_list	Array of strings	List of parameters after mapping orchestration. This parameter is mandatory when orchestration_strategy is set to list. The list length ranges from 0 to 3000. The value can contain 1 to 128 characters, including letters, digits, hyphens (-), and underscores (_). Minimum: 1 Maximum: 128 Array Length: 0 - 3000
map_param_range	OrchestrationMapParamRange object	This parameter is for mapping range configurations of parameters after orchestration and is mandatory if orchestration_strategy is range or hash_range.

Parameter	Type	Description
mapped_param_value	String	The parameter value after orchestration can contain 1 to 128 characters, including only letters and digits. This parameter is optional only when orchestration_strategy is set to hash, head_n, or tail_n, or is_preprocessing is set to false. Minimum: 0 Maximum: 128
intercept_length	Integer	Truncation length. The value ranges from 1 to 100. This parameter is mandatory when the policy type is head_n or tail_n. If the truncation length is greater than the parameter length, the parameter truncation result is a complete parameter. Minimum: 1 Maximum: 100

Table 4-2000 OrchestrationMapParamRange

Parameter	Type	Description
range_start	String	Range start value. The value is a string that can be converted to an integer. After the conversion, the value of range_start ranges from 0 to 9223372036854775807. And the value of range_start cannot be greater than that of range_end.
range_end	String	Range end value. The value is a string that can be converted to an integer. After the conversion, the value of range_end ranges from 0 to 9223372036854775807. And the value of range_start cannot be greater than that of range_end.

Status code: 400

Table 4-2001 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401**Table 4-2002** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-2003** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-2004** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-2005** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

Updating an orchestration rule

```
{
  "orchestration_name": "orchestration_demo_1",
  "orchestration_strategy": "range",
  "orchestration_mapped_param": {
    "mapped_param_name": "shared-tag",
    "mapped_param_type": "number",
    "mapped_param_location": "header"
  },
  "orchestration_map": [ {
    "map_param_range": {
      "range_start": "1",
      "range_end": "1000"
    },
    "mapped_param_value": "1"
  } ]
}
```

Example Responses

Status code: 200

OK

```
{
  "orchestration_id": "yt655e81d9cb4424bf704ef2b0ac7600",
  "orchestration_name": "orchestration_demo_1",
  "orchestration_create_time": "2023-07-02T12:31:23.353Z",
  "orchestration_update_time": "2023-07-02T13:31:23.353Z",
  "orchestration_strategy": "range",
  "orchestration_mapped_param": {
    "mapped_param_name": "shared-tag",
    "mapped_param_type": "number",
    "mapped_param_location": "header"
  },
  "orchestration_map": [ {
    "map_param_range": {
      "range_start": "1",
      "range_end": "1000"
    },
    "mapped_param_value": "1"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIG.2012",
  "error_msg": "Invalid parameter value,parameterName:orchestration_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
  "error_msg" : "The instance does not exist;id:f0fa1789-3b76-433b-a787-9892951c620ec"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.32.5 Deleting an Orchestration Rule

Function

This API is used to delete an orchestration rule.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/orchestrations/{orchestration_id}

Table 4-2006 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
orchestration_id	Yes	String	Orchestration rule ID.

Request Parameters

Table 4-2007 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-2008 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401

Table 4-2009 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-2010** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-2011** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-2012** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{  
  "error_code" : "APIG.2012",
```

```
{
  "error_msg": "Invalid parameter value,parameterName:orchestration_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIG.1002",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code": "APIG.1005",
  "error_msg": "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code": "APIG.3030",
  "error_msg": "The instance does not exist;id:f0fa1789-3b76-433b-a787-9892951c620ec"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code": "APIG.9999",
  "error_msg": "System error"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.32.6 Querying APIs to Which an Orchestration Rule Is Bound

Function

This API is used to query the APIs to which a specified plug-in has been bound.

- APIs bound with a specified plug-in
- Pagination query
- Fuzzy query by API name

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/orchestrations/
{orchestration_id}/attached-apis

Table 4-2013 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
orchestration_id	Yes	String	Orchestration rule ID.

Table 4-2014 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
api_name	No	String	API name.
api_id	No	String	App ID

Request Parameters

Table 4-2015 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-2016 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
apis	Array of OrchestrationApi Info objects	APIs to which an orchestration rule has been bound.

Table 4-2017 OrchestrationApiInfo

Parameter	Type	Description
api_id	String	API ID.
api_name	String	API name. Start with a letter or digit with 3 to 255 characters. Only letters, digits, and these special characters are allowed: - _./:()
req_method	String	Request method.
req_uri	String	Request address. It can contain request parameters enclosed with braces ({}). For example, /getUserInfo/{userId}. Special characters, such as asterisks (*), slashes (/), percent signs (%), hyphens (-), underscores (_), and periods (.), are allowed. It can contain a maximum of 512 characters and must comply with the URI specifications. Environment variables are supported. Each must start with a letter and can consist of 3 to 32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. NOTE The address must comply with the URI specifications.
auth_type	String	API authentication mode. Options: • NONE • APP • IAM • AUTHORIZER
match_mode	String	API matching mode. Options: • SWA: prefix match • NORMAL: normal match (absolute match) Default: NORMAL
group_id	String	ID of the API group to which an API belongs.
group_name	String	Name of the API group to which the API belongs.
attached_time	String	Binding time.

Status code: 400**Table 4-2018** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 401**Table 4-2019** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 403**Table 4-2020** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 404**Table 4-2021** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500**Table 4-2022** Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "apis" : [ {
    "api_id" : "8aa097b00e9843efabc9c593d11b769d",
    "api_name" : "api_demo",
    "req_method" : "GET",
    "req_uri" : "/test",
    "auth_type" : "IAM",
    "match_mode" : "NORMAL",
    "group_id" : "b9be707660c5406394f8973e087bae20",
    "group_name" : "group_demo",
    "attached_time" : "2023-07-02T12:31:23.353Z"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:instance_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIG.3030",
}
```

```
{  "error_msg" : "The instance does not exist;id:f0fa1789-3b76-433b-a787-9892951c620ec"}
```

Status code: 500

Internal Server Error

```
{  "error_code" : "APIG.9999",  "error_msg" : "System error"}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.33 Gateway Custom Inbound Port Management

4.33.1 Querying the Domain Name Bound to a Custom Inbound Port

Function

This API is used to query the domain name bound to a custom inbound port.

Calling Method

For details, see [Calling APIs](#).

URI

```
GET /v2/{project_id}/apigw/instances/{instance_id}/custom-ingress-ports/{ingress_port_id}/domains
```

Table 4-2023 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
ingress_port_id	Yes	String	Gateway inbound port ID.

Table 4-2024 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
domain_name	No	String	The domain name of the inbound port. Minimum: 0 Maximum: 255

Request Parameters

Table 4-2025 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200**Table 4-2026** Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.
total	Long	Number of resources that match the query conditions.
domain_infos	Array of PortBindingDomainInfo objects	Information list of domain names bound to the inbound port.

Table 4-2027 PortBindingDomainInfo

Parameter	Type	Description
group_id	String	ID of the API group to which the inbound port is bound. Minimum: 0 Maximum: 64
group_name	String	Name of the API group to which the inbound port is bound. Minimum: 3 Maximum: 255
domain_name	String	Domain names bound to the inbound port. Minimum: 0 Maximum: 255

Status code: 400**Table 4-2028** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-2029** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-2030** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-2031** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "domain_infos" : [ {
    "group_id" : "73c58022f20d495aa18885d718647f09",
    "group_name" : "group_01",
    "domain_name" : "test.com"
  } ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "APIG.2012",
  "error_msg" : "Invalid parameter value,parameterName:ingress_port_id. Please refer to the support documentation"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIG.1002",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIG.1005",
  "error_msg" : "No permissions to request this method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIG.9999",
  "error_msg" : "System error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.33.2 Querying the Custom Inbound Ports of a Gateway

Function

This API is used to query the custom inbound ports of a gateway.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v2/{project_id}/apigw/instances/{instance_id}/custom-ingress-ports

Table 4-2032 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Table 4-2033 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Long	Offset from which the query starts. If the value is less than 0, it is automatically converted to 0. Default: 0

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of items displayed on each page. A value less than or equal to 0 will be automatically converted to 20, and a value greater than 500 will be automatically converted to 500. Minimum: 1 Maximum: 500 Default: 20
protocol	No	String	Request protocol of inbound ports. • HTTP: The inbound port uses HTTP. • HTTPS: The inbound port uses HTTPS.
ingress_port	No	Integer	Inbound port number. The value ranges from 1024 to 49151. Minimum: 1024 Maximum: 49151

Request Parameters

Table 4-2034 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-2035 Response body parameters

Parameter	Type	Description
size	Integer	Length of the returned resource list.

Parameter	Type	Description
total	Long	Number of resources that match the query conditions.
ingress_port_infos	Array of IngressPortInfo objects	Custom inbound ports.

Table 4-2036 IngressPortInfo

Parameter	Type	Description
protocol	String	Custom inbound port protocol. • HTTP: The inbound port uses HTTP. • HTTPS: The inbound port uses HTTPS.
ingress_port	Integer	Inbound port number. The value ranges from 1024 to 49151. Minimum: 1024 Maximum: 49151
ingress_port_id	String	Inbound port ID. Minimum: 32 Maximum: 36
status	String	The status of the custom inbound port. • normal: The inbound port is normal. • abnormal: The inbound port is abnormal and cannot be used.

Status code: 401**Table 4-2037** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-2038 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-2039 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "size" : 1,
  "ingress_port_infos" : [ {
    "protocol" : "HTTP",
    "ingress_port" : 8080,
    "ingress_port_id" : "0ae98839d78043d8a6dff54d7cb096dc",
    "status" : "normal"
  } ]
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.33.3 Adding an Inbound Port for a Gateway

Function

This API is used to add an inbound port for a gateway. In the same gateway, a port can only support one protocol.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v2/{project_id}/apigw/instances/{instance_id}/custom-ingress-ports

Table 4-2040 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.

Request Parameters

Table 4-2041 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-2042 Request body parameters

Parameter	Mandatory	Type	Description
protocol	Yes	String	Custom inbound port protocol. • HTTP: The inbound port uses HTTP. • HTTPS: The inbound port uses HTTPS.
ingress_port	Yes	Integer	Inbound port number. The value ranges from 1024 to 49151. Minimum: 1024 Maximum: 49151

Response Parameters

Status code: 201

Table 4-2043 Response body parameters

Parameter	Type	Description
protocol	String	Custom inbound port protocol. • HTTP: The inbound port uses HTTP. • HTTPS: The inbound port uses HTTPS.
ingress_port	Integer	Inbound port number. The value ranges from 1024 to 49151. Minimum: 1024 Maximum: 49151

Parameter	Type	Description
ingress_port_id	String	Inbound port ID. Minimum: 32 Maximum: 36
status	String	The status of the custom inbound port. • normal: The inbound port is normal. • abnormal: The inbound port is abnormal and cannot be used.

Status code: 400**Table 4-2044** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401**Table 4-2045** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-2046** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404

Table 4-2047 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-2048** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Adding an inbound port for a gateway

```
{
  "protocol": "HTTP",
  "ingress_port": 8080
}
```

Example Responses

Status code: 201

Created

```
{
  "protocol": "HTTP",
  "ingress_port": 8080,
  "ingress_port_id": "0ae98839d78043d8a6dff54d7cb096dc",
  "status": "normal"
}
```

Status code: 400

Bad Request

```
{
  "error_code": "APIC.7211",
  "error_msg": "Parameter value does not match the rules, parameter name[protocol]"
}
```

Status code: 401

Unauthorized

```
{
  "error_code": "APIC.7102",
  "error_msg": "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7302",
  "error_msg" : "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

4.33.4 Deleting an Inbound Port of a Gateway

Function

This API is used to delete an inbound port of a gateway, not including ports 80 and 443.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v2/{project_id}/apigw/instances/{instance_id}/custom-ingress-ports/{ingress_port_id}

Table 4-2049 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain it, see Obtaining a Project ID .
instance_id	Yes	String	Gateway ID, which can be obtained from the gateway information on the APIG console.
ingress_port_id	Yes	String	Gateway inbound port ID.

Request Parameters

Table 4-2050 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-2051 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-2052 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403**Table 4-2053** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 404**Table 4-2054** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500**Table 4-2055** Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

None

Example Responses

Status code: 400

Bad Request

```
{  
  "error_code" : "APIC.7211",  
}
```

```
{
  "error_msg" : "Parameter value does not match the rules, parameter name[ingress_port_id]"
}
```

Status code: 401

Unauthorized

```
{
  "error_code" : "APIC.7102",
  "error_msg" : "Incorrect token or token resolution failed"
}
```

Status code: 403

Forbidden

```
{
  "error_code" : "APIC.7106",
  "error_msg" : "No permissions to request for the method"
}
```

Status code: 404

Not Found

```
{
  "error_code" : "APIC.7302",
  "error_msg" : "Instance not found"
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "APIC.9000",
  "error_msg" : "Failed to request internal service"
}
```

Status Codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See [Error Codes](#).

5 Shared Gateway APIs (for Existing Users)

5.1 API Group Management

5.1.1 Object Model

This section describes the object model for API groups.

 NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of **C** is mandatory.

Table 5-1 Object model for API groups

Parameter	Data Type	Description	Operation Type	Mandatory
ID	String	API group ID	R	-
NAME	String	API group name	CRU	Yes
STATUS	Integer	Status of the API group, which can be: • 1: normal • 2: disabled • 3: deleted Default value: 1 This parameter is not used currently.	R	-

Parameter	Data Type	Description	Operation Type	Mandatory
SL_DOMAIN	String	Subdomain name that APIG automatically allocates to the API group. The subdomain name cannot be modified.	R	-
SL_DOMAINS	Array of strings	List of subdomain names that APIG automatically allocates to the API group. These subdomain names cannot be modified.	R	-
PROJECT_ID	String	ID of the tenant that creates the API group, that is, the owner of the API group	-	-
DOMAIN_NAME	String	Name of the tenant that creates the API group	-	-
REGISTER_TIME	Timestamp	Time when the API group is created. The value of this parameter is generated by the system by default.	R	-
UPDATE_TIME	Timestamp	Time when the API group was last modified	R	-
REMARK	String	Description of the API group, such as functions and usage	CRU	No
THROTTLE_ID	String	ID of the request throttling policy that controls the number of times APIs in the API group can be accessed within a specified period NOTE The value of this parameter indicates the total number of times all APIs in the API group can be accessed within a specified period, and not the number of times each API can be accessed within the period.	RU	-

5.1.2 Creating an API Group

Function

This API is used to create an API group. An API group is an API management unit and the entry to a service. A subdomain name is returned as the access entry when an API group is created. APIs in an API group should be correlated with each other.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-2 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/api-groups

Request

Table 5-3 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	API group name An API group name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
remark	No	String	Description of the API group The description cannot exceed 255 characters.

Example request:

```
{
  "name": "api_group_001",
  "remark": "API group 1"
}
```

Response

Table 5-4 Parameter description

Parameter	Type	Description
id	String	API group ID
name	String	API group name
status	Integer	Status of the API group
sl_domain	String	Subdomain name that APIG automatically allocates to the API group
sl_domains	Array of strings	List of subdomain names that APIG automatically allocates to the API group
register_time	Timestamp	Time when the API group is created
update_time	Timestamp	Time when the API group was last modified
remark	String	Description of the API group
on_sell_status	Integer	Indicates whether the API group has been listed on KooGallery. The value can be: • 1: listed • 2: not listed • 3: under approval
call_limits	Integer	Total number of times all APIs in the API group can be accessed. Set this parameter while considering the payload capacity of the backend service. By default, there is no limit on the number of API calls.
time_interval	Integer	Period of time for limiting the number of API calls
time_unit	String	Time unit for limiting the number of API calls
url_domains	Array of UrlDomainsResp objects	List of independent domain names bound to the API group
is_default	Integer	Indicates whether the API group is the default API group. By default, the API group is not the default API group. The value can be: • 1: default API group • 2: non-default API group

Table 5-5 UrlDomainsResp

Parameter	Type	Description
id	String	Domain ID
domain	String	Domain name
cname_status	Integer	CNAME resolution status of the domain name, which can be: 1: not resolved 2: resolving 3: resolved 4: resolution failed
ssl_id	String	SSL certificate ID
ssl_name	String	SSL certificate name

Example response:

```
{
  "id": "7efb2b91-155a-4f6a-9f45-c5c95a6e4950",
  "name": "api_group_001",
  "status": 1,
  "sl_domain": "0e91b83b-0774-4e8e-b187-2d695ed4743b.apigw.example.com",
  "sl_domains": ["0e91b83b-0774-4e8e-b187-2d695ed4743b.apigw.example.com", "0e91b83b-0774-4e8e-b187-2d695ed4743b.apigw.example.cn"],
  "remark": "API group 1",
  "register_time": "2017-12-28T11:44:53.831282304Z",
  "update_time": "2017-12-28T11:44:53.831283436Z",
  "on_sell_status": 2,
  "is_default": 2
}
```

Status Codes

Table 5-6 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
500	Server Internal Error

5.1.3 Modifying an API Group

Function

This API is used to modify the attributes of an API group. Only the **name** and **remark** attributes of an API group can be modified.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-7 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/api-groups/{id}

The following table lists the parameter in the URI.

Table 5-8 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	API group ID

Request

Table 5-9 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	API group name An API group name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
remark	No	String	Description of the API group The description cannot exceed 255 characters.

Example request:

```
{
  "name": "api_group_001",
  "remark": "API group 001"
}
```

Response

Table 5-10 Parameter description

Parameter	Type	Description
id	String	API group ID
name	String	API group name
status	Integer	Status of the API group
sl_domain	String	Subdomain name that APIG automatically allocates to the API group
sl_domains	String	List of subdomain names that APIG automatically allocates to the API group
register_time	Timestamp	Time when the API group is created
update_time	Timestamp	Time when the API group was last modified
remark	String	Description of the API group
call_limits	Integer	Total number of times all APIs in the API group can be accessed. Set this parameter while considering the payload capacity of the backend service. By default, there is no limit on the number of API calls.
time_interval	Integer	Period of time for limiting the number of API calls
time_unit	String	Time unit for limiting the number of API calls
url_domains	Array of UrlDomainsResp objects	List of independent domain names bound to the API group
on_sell_status	Integer	Indicates whether the API group has been listed on KooGallery. The value can be: • 1: listed • 2: not listed • 3: under approval
is_default	Integer	Indicates whether the API group is the default API group. By default, the API group is not the default API group. The value can be: • 1: default API group • 2: non-default API group

Table 5-11 UrlDomainsResp

Parameter	Type	Description
id	String	Domain ID
domain	String	Domain name
cname_status	Integer	CNAME resolution status of the domain name, which can be: 1: not resolved 2: in progress 3: successful 4: failed
ssl_id	String	ID of the SSL certificate
ssl_name	String	Name of the SSL certificate

Example response:

```
{
  "id": "7efb2b91-155a-4f6a-9f45-c5c95a6e4950",
  "name": "api_group_001",
  "status": 1,
  "sl_domain": "0e91b83b-0774-4e8e-b187-2d695ed4743b.apigw.example.com",
  "sl_domains": ["0e91b83b-0774-4e8e-b187-2d695ed4743b.apigw.example.com", "0e91b83b-0774-4e8e-b187-2d695ed4743b.apigw.example.cn"],
  "remark": "API group 001",
  "register_time": "2017-12-28T11:44:53Z",
  "update_time": "2017-12-28T11:49:01.048600577Z",
  "on_sell_status": 2,
  "is_default": 2
}
```

Status Codes

Table 5-12 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
409	Conflict
500	Server Internal Error

5.1.4 Deleting an API Group

Function

This API is used to delete an API group.

If the group to delete contains APIs, take the APIs offline and delete them.

All resources (independent domain names, SSL certificates, and release information) directly or indirectly associated with the group will be deleted. The operation will unbind the external domain names from the subdomain name based on the CNAME resolution mode.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-13 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/api-groups/{id}

The following table lists the parameter in the URI.

Table 5-14 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	API group ID

Request

N/A

Response

N/A

Status Codes

Table 5-15 Status codes

Status Code	Description
204	No Content
401	Unauthorized

Status Code	Description
403	Forbidden
404	Not Found
409	Conflict
500	Server Internal Error

5.1.5 Querying Details of an API Group

Function

This API is used to query the details of an API group.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-16 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/api-groups/{id}

The following table lists the parameter in the URI.

Table 5-17 Parameter description

Parameter	Mandator y	Type	Description
id	Yes	String	API group ID

Request

N/A

Response

Table 5-18 Parameter description

Parameter	Type	Description
id	String	API group ID

Parameter	Type	Description
name	String	API group name
status	Integer	Status of the API group
sl_domain	String	Subdomain name that APIG automatically allocates to the API group
sl_domains	Array of strings	List of subdomain names that APIG automatically allocates to the API group
register_time	Timestamp	Time when the API group is created
update_time	Timestamp	Time when the API group was last modified
remark	String	Description of the API group
call_limits	Integer	Total number of times all APIs in the API group can be accessed. Set this parameter while considering the payload capacity of the backend service. By default, there is no limit on the number of API calls.
time_interval	Integer	Period of time for limiting the number of API calls
time_unit	String	Time unit for limiting the number of API calls
url_domains	Array of UrlDomainsResp objects	List of independent domain names bound to the API group
on_sell_status	Integer	Indicates whether the API group has been listed on KooGallery. The value can be: • 1: listed • 2: not listed • 3: under approval

Table 5-19 UrlDomainsResp

Parameter	Type	Description
id	String	Domain ID
domain	String	Domain name
cname_status	Integer	CNAME resolution status of the domain name, which can be: • 1: not resolved • 2: in progress • 3: successful • 4: failed

Parameter	Type	Description
ssl_id	String	SSL certificate ID
ssl_name	String	SSL certificate name

Example response:

```
{
  "id": "7efb2b91-155a-4f6a-9f45-c5c95a6e4950",
  "name": "api_group_001",
  "status": 1,
  "sl_domain": "0e91b83b-0774-4e8e-b187-2d695ed4743b.apigw.example.com",
  "sl_domains": ["0e91b83b-0774-4e8e-b187-2d695ed4743b.apigw.example.com", "0e91b83b-0774-4e8e-b187-2d695ed4743b.apigw.example.cn"],
  "remark": "API group 001",
  "register_time": "2017-12-28T11:44:53Z",
  "update_time": "2017-12-28T11:49:01.048601Z",
  "call_limits": 1000,
  "time_interval": 1,
  "time_unit": "SECOND",
  "on_sell_status": 2
}
```

Status Codes

Table 5-20 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.1.6 Querying the API Group List

Function

This API is used to query the API group list.

If the operation is performed by a tenant, all groups of the tenant are queried. If the operation is performed by a tenant administrator, the groups of all tenants are queried.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-21 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/api-groups[?page_size, page_no, id, name]

 NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **id**, **name**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-22 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	API group ID
name	No	String	API group name
page_size	No	Integer	Number of records displayed on each page. The default value is 20 . Maximum value: 500
page_no	No	Integer	Page number. The default value is 1 .
precise_search	No	String	Parameter name for exact matching

Request

N/A

Response

Table 5-23 Parameter description

Parameter	Type	Description
total	Integer	Number of API groups that match the query conditions

Parameter	Type	Description
size	Integer	Length of the returned API group list
groups	Dictionary	API group list

Table 5-24 API group parameter description

Parameter	Type	Description
id	String	API group ID
name	String	API group name
status	Integer	API group status
sl_domain	String	Subdomain name that APIG automatically allocates to the API group
sl_domains	Array of strings	List of subdomain names that APIG automatically allocates to the API group
register_time	Timestamp	Time when the API group is created
update_time	Timestamp	Time when the API group was last modified
remark	String	Description of the API group
on_sell_status	Integer	Indicates whether the API group has been listed on KooGallery. The value can be: • 1: listed • 2: not listed • 3: under approval
call_limits	Integer	Total number of times all APIs in the API group can be accessed. Set this parameter while considering the payload capacity of the backend service. By default, there is no limit on the number of API calls.
time_interval	Integer	Period of time for limiting the number of API calls
time_unit	String	Time unit for limiting the number of API calls
url_domains	Array of UrlDomainsResp objects	List of independent domain names bound to the API group

Table 5-25 UrlDomainsResp

Parameter	Type	Description
id	String	Domain ID
domain	String	Domain name
cname_status	Integer	CNAME resolution status of the domain name, which can be: • 1: not resolved • 2: resolving • 3: resolved • 4: resolution failed
ssl_id	String	SSL certificate ID
ssl_name	String	SSL certificate name

Example response:

```
{
  "total": 2,
  "size": 2,
  "groups": [{
    "id": "02a8ab3c-b278-4de5-a096-852829671ae7",
    "name": "api_group_002",
    "status": 1,
    "sl_domain": "19e62eca-43d9-4ce2-a478-b3f48e67fb91.apigw.example.com",
    "sl_domains": ["19e62eca-43d9-4ce2-a478-b3f48e67fb91.apigw.example.com", "19e62eca-43d9-4ce2-a478-b3f48e67fb91.apigw.example.cn"],
    "remark": "API group 002",
    "register_time": "2017-12-28T11:57:35Z",
    "update_time": "2017-12-28T11:57:35Z",
    "on_sell_status": 2
  },
  {
    "id": "73c58022-f20d-495a-a188-85d718647f09",
    "name": "api_group_001",
    "status": 1,
    "sl_domain": "c4c230d1-a8f2-4816-b9df-09ac5989180c.apigw.example.com",
    "sl_domains": ["c4c230d1-a8f2-4816-b9df-09ac5989180c.apigw.example.com", "c4c230d1-a8f2-4816-b9df-09ac5989180c.apigw.example.cn"],
    "remark": "API group 001",
    "register_time": "2017-12-28T11:57:27Z",
    "update_time": "2017-12-28T11:57:27Z",
    "on_sell_status": 2
  }
]}
```

Status Codes

Table 5-26 Status codes

Status Code	Description
200	OK

Status Code	Description
400	Bad Request
401	Unauthorized
500	Server Internal Error

5.2 API Management

5.2.1 Object Model

This section describes the API and backend service object models.

 NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of C is mandatory.

Table 5-27 API object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	API ID	R	-
name	String	API name	CRU	Yes
group_id	String	ID of the API group to which the API belongs	CR	Yes
type	Integer	Type of the API, which can be: • 1: public • 2: private	CRU	Yes
status	Integer	Status of the API, which can be: • 1: enabled • 2: disabled • 3: deleted Default value: 1 This parameter is not used currently.	R	-
version	String	Version of the API	CRU	No

Parameter	Type	Description	Operation Type	Mandatory
req_protocol	String	Request protocol, which can be: • HTTP • HTTPS • BOTH: The API can be accessed through both HTTP and HTTPS. Default value: HTTPS	CRU	No
req_method	String	Request method, which can be: • GET • POST • PUT • DELETE • HEAD • PATCH • OPTIONS • ANY	CRU	Yes
req_uri	String	Access address (URI) of the API, excluding the domain name, port number, and request protocol	CRU	Yes
auth_type	String	Security authentication mode, which can be: • NONE • APP • IAM • AUTHORIZER	CRU	Yes
authorizer_id	String	ID of the frontend custom authorizer	CRU	No
match_mode	String	Route matching mode, which can be: • SWA: prefix match • NORMAL: exact match	CRU	Yes

Parameter	Type	Description	Operation Type	Mandatory
arrange_necessary	Integer	Indicates whether orchestration is required. The value can be: • 1: yes • 2: no Default value: 2	R	-
backend_type	String	Backend type, which can be: • HTTP (web) • FUNCTION • MOCK	CRU	Yes
register_time	Timestamp	Time when the API was created	R	-
update_time	Timestamp	Time when the API was last modified	R	-
remark	String	Description of the API	CRU	No
tag	String	API tag	CRU	No
cors	String	Indicates whether cross-origin resource sharing (CORS) is supported • TRUE: supported • FALSE: not supported Default value: FALSE	CRU	No
response_id	String	ID of the custom response	CRU	No

Table 5-28 Web backend object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Web backend ID	R	-

Parameter	Type	Description	Operation Type	Mandatory
status	Integer	Status of the web backend, which can be: • 1: enabled • 2: disabled • 3: deleted Default value: 1 This parameter is not used currently.	R	-
version	String	Version of the web backend	CRU	No
url_domain	String	Backend endpoint	CRU	Yes
req_protocol	String	Request protocol, which can be: • HTTP • HTTPS	CRU	Yes
req_method	String	Request method, which can be: • GET • POST • PUT • DELETE • HEAD • PATCH • OPTIONS • ANY	CRU	Yes
req_uri	String	Access address (URI) of the web backend	CRU	Yes
timeout	Integer	Timeout duration in milliseconds. Range: 1–60,000.	CRU	Yes
front_api_id	String	API ID	R	-
register_time	Timestamp	Creation time	R	-
update_time	Timestamp	Time when the web backend was last modified	R	-
remark	String	Description of the web backend	CRU	No

Parameter	Type	Description	Operation Type	Mandatory
vpc_status	Integer	Indicates whether to use a VPC channel. The value can be: • 1: yes • 2: no	CRU	No. No VPC channel is used by default.
vpc_info	String	VPC channel information	CRU	No. This parameter is required only when vpc_status is set to 1 .
authorizer_id	String	ID of the backend custom authorizer	CRU	No

Table 5-29 Mock backend object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Mock backend ID	R	-
front_api_id	String	API ID	R	-
status	Integer	Status of the Mock backend, which can be: • 1: enabled • 2: disabled • 3: deleted Default value: 1 This parameter is not used currently.	R	-
version	String	Version of the Mock backend	CRU	No
result_content	String	Mock response	CRU	No

Parameter	Type	Description	Operation Type	Mandatory
register_time	Timestamp	Creation time	R	-
update_time	Timestamp	Time when the Mock backend was last modified	R	-
remark	String	Description of the Mock backend	CRU	No

Table 5-30 FunctionGraph backend object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Function ID	R	-
front_api_id	String	API ID	R	-
status	Integer	Status of the function, which can be: • 1: enabled • 2: disabled • 3: deleted Default value: 1 This parameter is not used currently.	R	-
version	String	Function version	CRU	No
function_urn	String	Function URN	CRU	Yes
invocation_type	String	Invocation mode, which can be async or sync	CRU	Yes
timeout	Integer	Timeout duration in milliseconds. Range: 1–60,000.	CRU	Yes
register_time	Date	Creation time	R	-
update_time	Date	Time when the function was last modified	R	-
remark	String	Description of the function	CRU	No

Table 5-31 Request parameter object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Parameter ID	R	-
front_api_id	String	API ID	R	-
name	String	Parameter name	CRU	Yes
type	String	Parameter type, which can be: • string • number	CRU	Yes
location	String	Parameter location, which can be: • PATH • QUERY • HEADER • FORMDATA	CRU	Yes
default_value	String	Default value	CRU	No
sample_value	String	Example value	CRU	No
required	Integer	Whether the parameter is mandatory • 1: yes • 2: no	CRU	Yes
valid_enable	Integer	Whether validity check is enabled • 1: yes • 2: no	CRU	Yes
remark	String	Parameter description	CRU	No
enumerations	String	Enumerated value	CRU	No
min_num	String	Minimum value	CRU	No
max_num	String	Maximum value	CRU	No
min_size	Integer	Minimum length	CRU	No
max_size	Integer	Maximum length	CRU	No
regular	String	Regular verification rule (currently not supported)	CRU	No
json_schema	String	JSON verification rule (currently not supported)	CRU	No

Table 5-32 Backend parameter object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Parameter ID	R	-
front_api_id	String	API ID	R	-
req_param_id	String	ID of the request parameter to which the backend parameter is mapped	R	-
name	String	Parameter name	CRU	Yes
location	String	Parameter location, which can be: • PATH • QUERY • HEADER • FORMDATA	CRU	Yes
origin	String	Parameter type, which can be: • REQUEST • CONSTANT • SYSTEM	CRU	Yes
value	String	Parameter value • If origin is set to REQUEST, the value is the name of the request parameter. • If origin is set to SYSTEM, the value is the name of the gateway parameter. • If origin is set to CONSTANT, the value is the real value of the backend parameter.	CRU	No
remark	String	Parameter description	CRU	No
policy_id	String	ID of the associated policy condition	CRU	No

Table 5-33 Web backend policy object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Backend ID	R	-
front_api_id	String	API ID	R	-
name	String	Backend name	CRU	Yes
url_domain	String	Backend endpoint	CRU	Yes
req_protocol	String	Request protocol, which can be: • HTTP • HTTPS	CRU	Yes
req_method	String	Request method, which can be: • GET • POST • PUT • DELETE • HEAD • PATCH • OPTIONS • ANY	CRU	Yes
req_uri	String	Access address (URI) of the web backend	CRU	Yes
timeout	Integer	Timeout duration in milliseconds. Range: 1–60,000.	CRU	No
vpc_status	Integer	Indicates whether to use a VPC channel. The value can be: • 1: yes • 2: no	CRU	No. No VPC channel is used by default.

Parameter	Type	Description	Operation Type	Mandatory
vpc_info	String	VPC channel information	CRU	No This parameter is required only when vpc_status is set to 1.
effect_mode	String	Effective mode of the backend policy • ALL • ANY	CRU	Yes

Table 5-34 Mock backend policy object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Backend ID	R	-
front_api_id	String	API ID	R	-
name	String	Backend name	CRU	Yes
result_content	String	Mock response	CRU	No
effect_mode	String	Effective mode of the backend policy • ALL • ANY	CRU	Yes

Table 5-35 FunctionGraph policy backend object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Backend ID	R	-
front_api_id	String	API ID	R	-
name	String	Backend name	CRU	Yes

Parameter	Type	Description	Operation Type	Mandatory
version	String	Function version	CRU	No
function_urn	String	Function URN	CRU	Yes
invocation_type	String	Invocation mode, which can be async or sync	CRU	Yes
timeout	Integer	Timeout duration in milliseconds. Range: 1–60,000.	CRU	Yes
effect_mode	String	Effective mode of the backend policy • ALL • ANY	CRU	Yes

Table 5-36 Backend policy condition object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Backend policy condition ID	R	-
condition_type	String	Condition type. Options: • exact: Exact match • enum: Enumeration • pattern: Regular expression	CRU	No
condition_value	String	Condition value	CRU	Yes
condition_origin	String	Condition source. Options: • param: Input parameter • source: Source IP address	CRU	Yes
req_param_id	String	Input parameter ID	R	-
policy_backend_id	String	Backend policy ID	CRU	Yes

Table 5-37 Authentication mode parameter object model

Parameter	Type	Description	Operation Type	Mandatory
app_code_auth_type	String	Indicates whether AppCode authentication is enabled. This parameter is valid only when auth_type is set to App . The default value is DISABLE . • DISABLE: AppCode authentication is disabled. • HEADER: AppCode authentication is enabled and the AppCode is located in the header.	CRU	-

5.2.2 Creating an API

Function

This API is used to register an API. API is an interface that encapsulates a set of service capabilities.

The definition of an API is divided into two parts. One part defines how the API is called by users, and the other part defines how APIG accesses the actual backend service requested by users.

APIG supports three backend types: HTTP/HTTPS web, FunctionGraph, and Mock.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-38 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/apis

Request

Table 5-39 Parameter description

Parameter	Mandatory	Type	Description
group_id	Yes	String	ID of the API group to which the API to be created will belong
name	Yes	String	API name An API name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
type	Yes	Integer	Indicates whether the API is available to the public. The value can be: • 1: public • 2: private
version	No	String	Version of the API A maximum of 16 characters are allowed.
req_protocol	No	String	Request protocol, which can be: • HTTP • HTTPS • BOTH: The API can be accessed through both HTTP and HTTPS. Default value: HTTPS
req_method	Yes	String	Request method, which can be: • GET • POST • PUT • DELETE • HEAD • PATCH • OPTIONS • ANY
req_uri	Yes	String	Access address NOTE The value of this parameter must comply with URI specifications.
match_mode	No	String	Route matching mode, which can be: • SWA: prefix match • NORMAL: exact match Default value: NORMAL

Parameter	Mandatory	Type	Description
remark	No	String	Description of the API The description cannot exceed 255 characters.
auth_type	Yes	String	Security authentication mode, which can be: • NONE • APP • IAM • AUTHORIZER
auth_opt	No	AuthOpt object	Security authentication mode parameter
authorizer_id	No	String	ID of the frontend custom authorizer
backend_type	Yes	String	Backend type, which can be: • HTTP: web backend • FUNCTION: FunctionGraph backend • MOCK: Mock backend
tag	No	String	Service name tag This field will be discarded.
tags	No	Array of string	API tags Optional. This parameter contains a service name tag and other tags. The service name tag must start with APIG-SN-. Other tags cannot start with APIG-SN-.
cors	No	Bool	Indicates whether CORS is supported. • TRUE: supported • FALSE: not supported Default value: FALSE
body_remark	No	String	Description of the API request body, which can be an example request body, media type, or parameter information The description cannot exceed 20,480 characters.
result_normal_sample	No	String	Example response for a successful request The length cannot exceed 20,480 characters.

Parameter	Mandatory	Type	Description
result_failure_sample	No	String	Example response for a failed request The length cannot exceed 20,480 characters.
response_id	No	String	ID of the custom response
backend_api	Required if backend_type is set to HTTP .	Dictionary	Web backend details
mock_info	Required if backend_type is set to MOCK .	Dictionary	Mock backend details
func_info	Required if backend_type is set to FUNCTION .	Dictionary	FunctionGraph backend details
req_params	No	Dictionary	Request parameter list
backend_params	No	Dictionary	Backend parameter list
policy_https	Optional if backend_type is set to HTTP .	Dictionary	Web backend policy list
policy_mocks	Optional if backend_type is set to MOCK .	Dictionary	Mock backend policy list

Parameter	Mandatory	Type	Description
policy_functions	Optional if backend_type is set to FUNCTION .	Dictionary	FunctionGraph backend policy list

Table 5-40 Parameter description of backend_api

Parameter	Mandatory	Type	Description
url_domain	Required when no VPC channel is used.	String	Backend service address An endpoint URL is in the format of "domain name (or IP address):port number", with up to 255 characters. For example, apig.example.com:7443. By default, the port number would be 443 for HTTPS or 80 for HTTP if it is not specified. An endpoint can contain environment variables, each starting with a letter and consisting of 3–32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed in environment variables.
version	No	String	Web backend version A maximum of 16 characters are allowed.
req_protocol	Yes	String	Request protocol, which can be: • HTTP • HTTPS
req_method	Yes	String	Request method, which can be: • GET • POST • PUT • DELETE • HEAD • PATCH • OPTIONS • ANY

Parameter	Mandatory	Type	Description
req_uri	Yes	String	Request address A request address can contain up to 512 characters and must comply with URI specifications. The request address can contain environment variables, each starting with a letter and consisting of 3–32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed in environment variables. NOTE The value of this parameter must comply with URI specifications.
timeout	Yes	Integer	Timeout duration for APIG to request for the backend service. Range: 1–60,000. Unit: ms.
remark	No	String	Description of the backend service The description cannot exceed 255 characters.
vpc_status	No	Integer	Indicates whether to use a VPC channel. The value can be: • 1: yes • 2: no
vpc_info	Required when vpc_status is set to 1.	Dictionary	VPC channel details
authorizer_id	No	String	ID of the backend custom authorizer

Table 5-41 VPC channel parameter description

Parameter	Mandatory	Type	Description
vpc_id	Yes	String	VPC channel ID
vpc_proxy_host	No	String	Proxy host

Table 5-42 Parameter description of mock_info

Parameter	Mandatory	Type	Description
result_content	No	String	Mock response
version	No	String	Version of the Mock backend A maximum of 64 characters are allowed.
remark	No	String	Description of the Mock backend The description cannot exceed 255 characters.

Table 5-43 Parameter description of func_info

Parameter	Mandatory	Type	Description
function_urn	Yes	String	Function URN
invocation_type	Yes	String	Invocation mode, which can be async or sync
timeout	Yes	Integer	Timeout duration for APIG to request for FunctionGraph. Range: 1–60,000. Unit: ms.
version	No	String	Function version A maximum of 64 characters are allowed.
remark	No	String	Description of the function The description cannot exceed 255 characters.

Table 5-44 Parameter description of req_params

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name A parameter name consists of 1–32 characters, starting with a letter. Only letters, digits, periods (.), hyphens (-), and underscores (_) are allowed.

Parameter	Mandatory	Type	Description
type	Yes	String	Parameter type, which can be: • STRING • NUMBER
location	Yes	String	Parameter location, which can be: • PATH • QUERY • HEADER
default_value	No	String	Default value
sample_value	No	String	Example value
required	No	Integer	Indicates whether the parameter is mandatory. • 1: yes • 2: no The value of this parameter is 1 if Location is set to PATH and 2 if Location is set to another value.
valid_enable	No	Integer	Indicates whether validity check is enabled. • 1: enabled • 2: disabled The default value is 2 .
remark	No	String	Description of the parameter The description cannot exceed 255 characters.
enumerations	No	String	Enumerated value
min_num	No	Integer	Minimum value, which is valid when the parameter type is NUMBER
max_num	No	Integer	Maximum value, which is valid when the parameter type is NUMBER
min_size	No	Integer	Minimum length
max_size	No	Integer	Maximum length
regular	No	String	Regular verification rule (currently not supported)
json_schema	No	String	JSON verification rule (currently not supported)

Table 5-45 Parameter description of backend_params

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name A parameter name consists of 1–32 characters, starting with a letter. Only letters, digits, periods (.), hyphens (-), and underscores (_) are allowed.
location	Yes	String	Parameter location, which can be: • PATH • QUERY • HEADER
origin	Yes	String	Parameter type, which can be: • REQUEST • CONSTANT • SYSTEM
value	Yes	String	Parameter value, which can contain no more than 255 characters If origin is set to REQUEST , the value is the parameter name in req_params . If origin is set to CONSTANT , the value is the real value of the backend parameter. If origin is set to SYSTEM , the value is the name of the gateway parameter.
remark	No	String	Description of the parameter The description cannot exceed 255 characters.

Table 5-46 Parameter description of policy_https

Parameter	Mandatory	Type	Description
name	Yes	String	Backend name A backend name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.

Parameter	Mandatory	Type	Description
url_domain	Required when no VPC channel is used.	String	Endpoint of the policy backend An endpoint consists of a domain name or IP address and a port number, with not more than 255 characters. It must be in the format "<i>Domain name:Port number</i>", for example, apig.example.com:7443. By default, the port number would be 443 for HTTPS or 80 for HTTP if it is not specified. An endpoint can contain environment variables, each starting with a letter and consisting of 3–32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed in environment variables.
req_protocol	Yes	String	Request protocol, which can be: • HTTP • HTTPS
req_method	Yes	String	Request method, which can be: • GET • POST • PUT • DELETE • HEAD • PATCH • OPTIONS • ANY
req_uri	Yes	String	Request address A request address can contain up to 512 characters and must comply with URI specifications. The request address can contain environment variables, each starting with a letter and consisting of 3–32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed in environment variables. NOTE The value of this parameter must comply with URI specifications.
timeout	No	Integer	Timeout duration for APIG to request for the backend service. Range: 1–60,000. Unit: ms.

Parameter	Mandatory	Type	Description
vpc_status	No	Integer	Indicates whether to use a VPC channel. The value can be: • 1: yes • 2: no
vpc_info	Required when vpc_status is set to 1.	Dictionary	VPC channel details
effect_mode	Yes	String	Effective mode of the backend policy • ALL • ANY
conditions	Yes	Dictionary	Policy condition list
backend_params	No	Dictionary	Backend parameter list

Table 5-47 Parameter description of policy_mock

Parameter	Mandatory	Type	Description
name	Yes	String	Backend name A backend name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
result_content	No	String	Mock response
effect_mode	Yes	String	Effective mode of the backend policy • ALL • ANY
conditions	Yes	Dictionary	Policy condition list
backend_params	No	Dictionary	Backend parameter list

Table 5-48 Parameter description of policy_functions

Parameter	Mandatory	Type	Description
name	Yes	String	Backend name A backend name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
function_urn	Yes	String	Function URN
invocation_type	Yes	String	Invocation mode. Options: • async: asynchronous • sync: synchronous
timeout	No	Integer	Timeout duration for APIG to request for FunctionGraph. Range: 1–60,000. Unit: ms.
version	No	String	Function version A maximum of 64 characters are allowed.
effect_mode	Yes	String	Effective mode of the backend policy • ALL • ANY
conditions	Yes	Dictionary	Policy condition list
backend_params	No	Dictionary	Backend parameter list

Table 5-49 Parameter description of conditions

Parameter	Mandatory	Type	Description
condition_type	Mandatory if the policy type is param .	String	Condition type. Options: • exact: Exact match • enum: Enumeration • pattern: Regular expression
condition_value	Yes	String	Condition value

Parameter	Mandatory	Type	Description
condition_origin	Yes	String	Condition source. Options: • param: Input parameter • source: Source IP address
req_param_name	Mandatory if the policy type is param .	String	Input parameter name

Table 5-50 AuthOpt

Parameter	Mandatory	Type	Description
app_code_auth_type	No	String	Indicates whether AppCode authentication is enabled. This parameter is valid only when auth_type is set to App . The default value is DISABLE . • DISABLE: AppCode authentication is disabled. • HEADER: AppCode authentication is enabled and the AppCode is located in the header.

Example request:

```
{
  "auth_type": "app",
  "auth_opt": {
    "app_code_auth_type": "HEADER"
  },
  "backend_api": {
    "req_method": "get",
    "req_protocol": "http",
    "req_uri": "/test",
    "timeout": 1000,
    "url_domain": "xxxxxxxxxx"
  },
  "backend_params": [
    {
      "location": "query",
      "name": "project_id",
      "origin": "request",
      "value": "project_id"
    },
    {
      "location": "query",
      "name": "city",
      "origin": "request",

```

```
    "value": "city"
  }
],
"backend_type": "http",
"group_id": "f71f69876f90456ca6fd18ed012fdc11",
"name": "test",
"req_method": "get",
"req_params": [
  {
    "location": "path",
    "name": "project_id",
    "required": 1,
    "type": "string"
  },
  {
    "location": "query",
    "name": "city",
    "required": 2,
    "type": "string"
  }
],
"req_uri": "/test/{project_id}",
"tags": ["APIG-SN-test", "test"],
"type": 1,
"result_normal_sample": "hello world!"
}
```

Response

Table 5-51 Parameter description

Parameter	Type	Description
id	String	API ID
name	String	API name
group_id	String	ID of the API group to which the API belongs
group_name	String	Name of the API group to which the API belongs
status	Integer	API status
type	Integer	API type
version	String	API version
req_protocol	String	Request protocol
req_method	String	Request method
req_uri	String	Access address
auth_type	String	Security authentication mode
auth_opt	Object	Security authentication mode parameter
match_mode	String	Matching mode
register_time	Timestamp	Time when the API was created
update_time	Timestamp	Time when the API was last modified

Parameter	Type	Description
remark	String	API description
backend_type	String	Backend type
arrange_necessary	Integer	Indicates whether orchestration is required.
tag	String	Service name tag, which is to be discarded
tags	[]String	API tags
cors	Bool	Indicates whether CORS is supported.
body_remark	String	Description of the API request body, which can be an example request body, media type, or parameter information
result_normal_sample	String	Example response for a successful request
result_failure_sample	String	Example response for a failed request
response_id	String	ID of the gateway response
backend_api	Dictionary	Web backend details
mock_info	Dictionary	Mock backend details
func_info	Dictionary	FunctionGraph backend details
req_params	Dictionary	Request parameter list
backend_params	Dictionary	Backend parameter list
policy_https	Dictionary	Web backend policy list
policy_mocks	Dictionary	Mock backend policy list
policy_functions	Dictionary	FunctionGraph backend policy list

Table 5-52 Parameter description of backend_api

Parameter	Type	Description
id	String	Backend ID
status	Integer	Web backend status
url_domain	String	Backend endpoint
version	String	Web backend version

Parameter	Type	Description
req_protocol	String	Request protocol
req_method	String	Request method
req_uri	String	Access address
timeout	Integer	Timeout duration in milliseconds
register_time	Timestamp	Creation time
update_time	Timestamp	Time when the web backend was last modified
remark	String	Description of the web backend
vpc_status	String	Indicates whether to use a VPC channel.
vpc_info	String	VPC channel information

Table 5-53 Parameter description of mock_info

Parameter	Type	Description
id	String	Mock backend ID
status	Integer	Mock backend status
version	String	Mock backend version
result_content	String	Mock response
register_time	Timestamp	Creation time
update_time	Timestamp	Time when the Mock backend was last modified
remark	String	Description of the Mock backend

Table 5-54 Parameter description of func_info

Parameter	Type	Description
id	String	Function ID
status	Integer	Function status
version	String	Function version
function_urn	String	Function URN
invocation_type	String	Invocation mode, which can be async or sync
register_time	Timestamp	Creation time

Parameter	Type	Description
update_time	Timestamp	Time when the function was last updated
timeout	Integer	Timeout duration in milliseconds
remark	String	Description of the function

Table 5-55 Parameter description of req_params

Parameter	Type	Description
id	String	Parameter ID
name	String	Parameter name
type	String	Parameter type
location	String	Parameter location
default_value	String	Default value
sample_value	String	Example value
required	Integer	Indicates whether the parameter is mandatory.
valid_enable	Integer	Indicates whether validity check is enabled.
remark	String	Description of the parameter
enumerations	String	Enumerated value
min_num	Integer	Minimum value, which is valid when the parameter type is NUMBER
max_num	Integer	Maximum value, which is valid when the parameter type is NUMBER
min_size	Integer	Minimum length
max_size	Integer	Maximum length
regular	String	Regular verification rule (currently not supported)
json_schema	String	JSON verification rule (currently not supported)

Table 5-56 Parameter description of backend_params

Parameter	Type	Description
id	String	Parameter ID

Parameter	Type	Description
req_param_id	String	ID of the request parameter to which the backend parameter is mapped
name	String	Parameter name
location	String	Parameter location
origin	String	Parameter type
value	String	Parameter value
remark	String	Description of the backend parameter

Table 5-57 Parameter description of policy_https

Parameter	Type	Description
id	String	Backend policy ID
name	String	Backend name
url_domain	String	Endpoint of the policy backend
req_protocol	String	Request protocol
req_method	String	Request method
req_uri	String	Access address
timeout	Integer	Timeout duration in milliseconds
vpc_status	String	Indicates whether to use a VPC channel.
vpc_info	String	VPC channel information
effect_mode	String	Effective mode of the backend policy
conditions	Dictionary	Policy condition list
backend_params	Dictionary	Backend parameter list

Table 5-58 Parameter description of policy_mock

Parameter	Type	Description
id	String	Backend policy ID
name	String	Backend name
result_content	String	Mock response
effect_mode	String	Effective mode of the backend policy

Parameter	Type	Description
conditions	Dictionary	Policy condition list
backend_params	Dictionary	Backend parameter list

Table 5-59 Parameter description of policy_functions

Parameter	Type	Description
id	String	Backend policy ID
name	String	Backend name
version	String	Function version
function_urn	String	Function URN
invocation_type	String	Invocation mode, which can be async or sync
timeout	Integer	Timeout duration in milliseconds
effect_mode	String	Effective mode of the backend policy
conditions	Dictionary	Policy condition list
backend_params	Dictionary	Backend parameter list

Table 5-60 Parameter description of conditions

Parameter	Type	Description
id	String	Backend policy condition ID
condition_type	String	Condition type
condition_value	String	Condition value
condition_origin	String	Condition source
req_param_name	String	Input parameter name
req_param_id	String	Input parameter ID
req_param_location	String	Input parameter location

Table 5-61 Parameter description of auth_opt

Parameter	Type	Description
app_code_auth_type	String	Indicates whether AppCode authentication is enabled.

Example response:

```
{
  "name": "test",
  "type": 1,
  "version": "V0.0.1",
  "req_protocol": "HTTPS",
  "req_method": "GET",
  "req_uri": "/test/{tenant_id}",
  "auth_type": "APP",
  "auth_opt": {
    "app_code_auth_type": "HEADER"
  },
  "tags": ["APIG-SN-test", "test"],
  "cors": false,
  "match_mode": "NORMAL",
  "backend_type": "HTTP",
  "group_id": "f71f69876f90456ca6fd18ed012fdc11",
  "result_normal_sample": "hello world!",
  "id": "81efcd94b8747a0b21e8c04144a4e8c",
  "status": 1,
  "arrange_necessary": 2,
  "register_time": "2018-08-15T03:41:11.0239936Z",
  "update_time": "2018-08-15T03:41:11.0239936Z",
  "group_name": "group0002",
  "backend_api": {
    "url_domain": "xxxxxxxxxx",
    "req_protocol": "HTTP",
    "req_method": "GET",
    "req_uri": "/test",
    "timeout": 1000,
    "vpc_status": 2,
    "id": "3442ffd031814e3a8f133a9f1ea08453",
    "status": 1,
    "register_time": "2018-08-15T03:41:11.1019236Z",
    "update_time": "2018-08-15T03:41:11.1019236Z"
  },
  "req_params": [
    {
      "name": "tenant_id",
      "type": "STRING",
      "location": "PATH",
      "required": 1,
      "valid_enable": 2,
      "id": "593c5560e0924e00af08fb458f850ecb"
    },
    {
      "name": "city",
      "type": "STRING",
      "location": "QUERY",
      "required": 2,
      "valid_enable": 2,
      "id": "e0b91bc81ae54f8ea850848d782d6e1e"
    }
  ],
  "backend_params": [
    {
      "name": "tenant_id",
```

```
    "location": "QUERY",
    "origin": "REQUEST",
    "value": "tenant_id",
    "id": "44e03de2351e43a8b18ba9ec1e71d2e9",
    "req_param_id": "593c5560e0924e00af08fb458f850ecb"
  },
  {
    "name": "city",
    "location": "QUERY",
    "origin": "REQUEST",
    "value": "city",
    "id": "b60fbc5b86f4f5c8705c445b9bd6325",
    "req_param_id": "e0b91bc81ae54f8ea850848d782d6e1e"
  }
],
"policy_https": [{
  "conditions": [{
    "id": "44e03de2351e43a8b18ba9ec1e71d2e9",
    "condition_type": "pattern",
    "condition_value": "^^[0-9]$",
    "condition_origin": "param",
    "req_param_name": "project_id",
    "req_param_id": "b60fbc5b86f4f5c8705c445b9sda325",
    "req_param_location": "PATH"
  }],
  "backend_params": [{
    "name": "project_id",
    "value": "bbbb",
    "location": "QUERY",
    "origin": "REQUEST",
    "id": "44e03de2351e43a8b18ba9ec1e71d2e8",
    "req_param_id": "593c5560e0924e00af08fb458f850ecb"
  }],
  "effect_mode": "ANY",
  "id": "44e03de2351e43a8b18ba9ec1e71d2e8",
  "name": "policy001",
  "req_method": "GET",
  "req_protocol": "http",
  "req_uri": "/test/policy",
  "timeout": 10000,
  "url_domain": "xxxxxxxxxx",
  "vpc_status": 2
}]
}
```

Status Codes

Table 5-62 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.2.3 Modifying an API

Function

This API is used to modify the information about an API, including its backend information.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-63 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/apis/{id}

The following table lists the parameter in the URI.

Table 5-64 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	API ID, which can be obtained by querying the API information

Request

Table 5-65 Parameter description

Parameter	Mandatory	Type	Description
group_id	No	String	ID of the API group to which the API belongs. The value of this parameter cannot be modified.
name	Yes	String	API name An API name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
type	Yes	Integer	Indicates whether the API is available to the public. The value can be: 1: public 2: private

Parameter	Mandatory	Type	Description
version	No	String	Version of the API A maximum of 16 characters are allowed.
req_protocol	No	String	Request protocol, which can be: • HTTP • HTTPS • BOTH: The API can be accessed through both HTTP and HTTPS. • WEBSOCKET Default value: HTTPS
req_method	Yes	String	Request method, which can be: • GET • POST • PUT • DELETE • HEAD • PATCH • OPTIONS • ANY
req_uri	Yes	String	Access address NOTE The value of this parameter must comply with URI specifications.
match_mode	No	String	Route matching mode, which can be: • SWA: prefix match • NORMAL: exact match Default value: NORMAL
remark	No	String	Description of the API The description cannot exceed 255 characters.
auth_type	Yes	String	Security authentication mode, which can be: • NONE • APP • IAM • AUTHORIZER
auth_opt	No	Dictionary	Security authentication mode parameter

Parameter	Mandatory	Type	Description
authorizer_id	No	String	ID of the frontend custom authorizer
backend_type	Yes	String	Backend type, which can be: • HTTP: web backend • FUNCTION: FunctionGraph backend • MOCK: Mock backend
tag	No	String	Service name tag This field will be discarded.
tags	No	[]String	API tags Optional. This parameter contains a service name tag and other tags. The service name tag must start with APIG-SN-. Other tags cannot start with APIG-SN-.
cors	No	Bool	Indicates whether CORS is supported. • TRUE: supported • FALSE: not supported Default value: FALSE
body_remark	No	String	Description of the API request body, which can be an example request body, media type, or parameter information The description cannot exceed 20,480 characters.
result_normal_sample	No	String	Example response for a successful request The length cannot exceed 20,480 characters.
result_failure_sample	No	String	Example response for a failed request The length cannot exceed 20,480 characters.
response_id	No	String	ID of the gateway response
backend_api	Required if backend_type is set to HTTP .	Dictionary	Web backend details

Parameter	Mandatory	Type	Description
mock_info	Required if backend_type is set to MOCK .	Dictionary	Mock backend details
func_info	Required if backend_type is set to FUNCTION .	Dictionary	FunctionGraph backend details
req_params	No	Dictionary	Request parameter list
backend_params	No	Dictionary	Backend parameter list
policy_https	Optional if backend_type is set to HTTP .	Dictionary	Web backend policy list
policy_mocks	Optional if backend_type is set to MOCK .	Dictionary	Mock backend policy list
policy_functions	Optional if backend_type is set to FUNCTION .	Dictionary	FunctionGraph backend policy list

Table 5-66 Parameter description of backend_api

Parameter	Mandatory	Type	Description
url_domain	Required when no VPC channel is used.	String	Backend endpoint An endpoint URL is in the format of "domain name (or IP address):port number", with up to 255 characters. For example, apig.example.com:7443 . By default, the port number would be 443 for HTTPS or 80 for HTTP if it is not specified. An endpoint can contain environment variables, each starting with a letter and consisting of 3–32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed in environment variables.
version	No	String	Web backend version A maximum of 16 characters are allowed.
req_protocol	Yes	String	Request protocol, which can be: • HTTP • HTTPS
req_method	Yes	String	Request method, which can be: • GET • POST • PUT • DELETE • HEAD • PATCH • OPTIONS • ANY
req_uri	Yes	String	Request address NOTE The value of this parameter must comply with URI specifications.
timeout	Yes	Integer	Timeout duration for APIG to request for the backend service. Range: 1–60,000. Unit: ms. Default value: 45000 . This value will be used if the specified value is outside the allowable range.
remark	No	String	Description of the web backend The description cannot exceed 255 characters.

Parameter	Mandatory	Type	Description
vpc_status	No	Integer	Indicates whether to use a VPC channel. The value can be: • 1: yes • 2: no
vpc_info	Required if vpc_status is set to 1.	Dictionary	VPC channel details
authorizer_id	No	String	ID of the backend custom authorizer

Table 5-67 VPC channel parameter description

Parameter	Mandatory	Type	Description
vpc_id	Yes	String	VPC channel ID
vpc_proxy_host	No	String	Proxy host

Table 5-68 Parameter description of mock_info

Parameter	Mandatory	Type	Description
result_content	No	String	Mock response
version	No	String	Version of the Mock backend A maximum of 64 characters are allowed.
remark	No	String	Description of the Mock backend The description cannot exceed 255 characters.

Table 5-69 Parameter description of func_info

Parameter	Mandatory	Type	Description
function_urn	Yes	String	Function URN
invocation_type	Yes	String	Invocation mode, which can be async or sync
timeout	Yes	Integer	Timeout duration for APIG to request for FunctionGraph. Range: 1–60,000. Unit: ms. Default value: 45000 . This value will be used if the specified value is outside the allowable range.
version	No	String	Function version A maximum of 64 characters are allowed.
remark	No	String	Description of the function The description cannot exceed 255 characters.

Table 5-70 Parameter description of req_params

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name A parameter name consists of 1–32 characters, starting with a letter. Only letters, digits, periods (.), hyphens (-), and underscores (_) are allowed.
type	Yes	String	Parameter type, which can be: • STRING • NUMBER
location	Yes	String	Parameter location, which can be: • PATH • QUERY • HEADER
default_value	No	String	Default value
sample_value	No	String	Example value

Parameter	Mandatory	Type	Description
required	No	Integer	Indicates whether the parameter is mandatory. • 1: yes • 2: no The value of this parameter is 1 if Location is set to PATH and 2 if Location is set to another value.
valid_enable	No	Integer	Indicates whether validity check is enabled. • 1: enabled • 2: disabled The default value is 2.
remark	No	String	Description of the parameter The description cannot exceed 255 characters.
enumerations	No	String	Enumerated value
min_num	No	Integer	Minimum value, which is valid when the parameter type is NUMBER
max_num	No	Integer	Maximum value, which is valid when the parameter type is NUMBER
min_size	No	Integer	Minimum length
max_size	No	Integer	Maximum length
regular	No	String	Regular verification rule (currently not supported)
json_schema	No	String	JSON verification rule (currently not supported)

Table 5-71 Parameter description of backend_params

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name A parameter name consists of 1–32 characters, starting with a letter. Only letters, digits, periods (.), hyphens (-), and underscores (_) are allowed.

Parameter	Mandatory	Type	Description
location	Yes	String	Parameter location, which can be: • PATH • QUERY • HEADER
origin	Yes	String	Parameter type, which can be: • REQUEST • CONSTANT • SYSTEM
value	Yes	String	Parameter value, which can contain not more than 255 characters If origin is set to REQUEST , the value is the parameter name in req_params . If origin is set to CONSTANT , the value is the real value of the backend parameter. If origin is set to SYSTEM , the value is the name of the gateway parameter.
remark	No	String	Description of the parameter The description cannot exceed 255 characters.

Table 5-72 Parameter description of policy_https

Parameter	Mandatory	Type	Description
name	Yes	String	Backend name A backend name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.

Parameter	Mandatory	Type	Description
url_domain	Required when no VPC channel is used.	String	Endpoint of the policy backend An endpoint consists of a domain name or IP address and a port number, with not more than 255 characters. It must be in the format "<i>Domain name:Port number</i>", for example, apig.example.com:7443. By default, the port number would be 443 for HTTPS or 80 for HTTP if it is not specified. An endpoint can contain environment variables, each starting with a letter and consisting of 3–32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed in environment variables.
req_protocol	Yes	String	Request protocol, which can be: • HTTP • HTTPS
req_method	Yes	String	Request method, which can be: • GET • POST • PUT • DELETE • HEAD • PATCH • OPTIONS • ANY
req_uri	Yes	String	Request address A request address can contain up to 512 characters and must comply with URI specifications. The request address can contain environment variables, each starting with a letter and consisting of 3–32 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed in environment variables. NOTE The value of this parameter must comply with URI specifications.

Parameter	Mandatory	Type	Description
timeout	No	Integer	Timeout duration for APIG to request for the backend service. Range: 1–60,000. Unit: ms. Default value: 45000 . This value will be used if the specified value is outside the allowable range.
vpc_status	No	Integer	Indicates whether to use a VPC channel. The value can be: • 1: yes • 2: no
vpc_info	Required if vpc_status is set to 1.	Dictionary	VPC channel details
effect_mode	Yes	String	Effective mode of the backend policy • ALL • ANY
conditions	Yes	Dictionary	Policy condition list
backend_params	No	Dictionary	Backend parameter list

Table 5-73 Parameter description of policy_mocks

Parameter	Mandatory	Type	Description
name	Yes	String	Backend name A backend name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
result_content	No	String	Mock response
effect_mode	Yes	String	Effective mode of the backend policy • ALL • ANY
conditions	Yes	Dictionary	Policy condition list

Parameter	Mandatory	Type	Description
backend_params	No	Dictionary	Backend parameter list

Table 5-74 Parameter description of policy_functions

Parameter	Mandatory	Type	Description
name	Yes	String	Backend name A backend name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
function_urn	Yes	String	Function URN
invocation_type	Yes	String	Invocation mode, which can be async or sync
timeout	No	Integer	Timeout duration for APIG to request for FunctionGraph. Range: 1–60,000. Unit: ms. Default value: 45000 . This value will be used if the specified value is outside the allowable range.
version	No	String	Function version A maximum of 64 characters are allowed.
effect_mode	Yes	String	Effective mode of the backend policy - ALL - ANY
conditions	Yes	Dictionary	Policy condition list
backend_params	No	Dictionary	Backend parameter list

Table 5-75 Parameter description of conditions

Parameter	Mandatory	Type	Description
condition_type	Mandatory if the policy type is param .	String	Condition type. Options: • exact: Exact match • enum: Enumeration • pattern: Regular expression
condition_value	Yes	String	Condition value
condition_origin	Yes	String	Condition source. Options: • param: Input parameter • source: Source IP address
req_param_name	Mandatory if the policy type is param .	String	Input parameter name

Table 5-76 Parameter description of auth_opt

Parameter	Mandatory	Type	Description
app_code_auth_type	No	String	Indicates whether AppCode authentication is enabled. This parameter is valid only when auth_type is set to App . The default value is DISABLE . • DISABLE: AppCode authentication is disabled. • HEADER: AppCode authentication is enabled and the AppCode is located in the header.

Example request:

```
{
  "auth_type": "app",
  "auth_opt": {
    "app_code_auth_type": "HEADER"
  },
  "backend_api": {
    "req_method": "get",
    "req_protocol": "http",
    "req_uri": "/test",
    "timeout": 1000,
    "url_domain": "xxxxxxxxx"
  }
}
```

```
},
"backend_params": [
  {
    "location": "query",
    "name": "project_id",
    "origin": "request",
    "value": "project_id"
  },
  {
    "location": "query",
    "name": "city",
    "origin": "request",
    "value": "city"
  }
],
"backend_type": "http",
"group_id": "f71f69876f90456ca6fd18ed012fdc11",
"name": "test",
"req_method": "get",
"req_params": [
  {
    "location": "path",
    "name": "project_id",
    "required": 1,
    "type": "string"
  },
  {
    "location": "query",
    "name": "city",
    "required": 2,
    "type": "string"
  }
],
"req_uri": "/test/{project_id}",
"tags": ["APIG-SN-test", "test"],
"type": 1,
"result_normal_sample": "hello world!"
}
```

Response

Table 5-77 Parameter description

Parameter	Type	Description
id	String	API ID
name	String	API name
group_id	String	ID of the API group to which the API belongs
group_name	String	Name of the API group to which the API belongs
status	Integer	API status
type	Integer	API type
version	String	API version
req_protocol	String	Request protocol
req_method	String	Request method

Parameter	Type	Description
req_uri	String	Access address
auth_type	String	Security authentication mode
auth_opt	Object	Security authentication mode parameter
match_mode	String	Matching mode
register_time	Timestamp	Time when the API was created
update_time	Timestamp	Time when the API was last modified
remark	String	Description of the API
backend_type	String	Backend type
run_env_name	String	Name of the environment in which the API has been published
run_env_id	String	ID of the environment in which the API has been published
publish_id	String	ID of the publication record
arrange_necessary	Integer	Indicates whether orchestration is required.
tag	String	Service name tag, which is to be discarded
tags	[]String	API tags
cors	Bool	Indicates whether CORS is supported.
body_remark	String	Description of the API request body, which can be an example request body, media type, or parameter information
result_normal_sample	String	Example response for a successful request
result_failure_sample	String	Example response for a failed request
response_id	String	ID of the gateway response
backend_api	Dictionary	Web backend details
mock_info	Dictionary	Mock backend details
func_info	Dictionary	FunctionGraph backend details
req_params	Dictionary	Request parameter list
backend_params	Dictionary	Backend parameter list
policy_https	Dictionary	Web backend policy list

Parameter	Type	Description
policy_mocks	Dictionary	Mock backend policy list
policy_functions	Dictionary	FunctionGraph backend policy list

Table 5-78 Parameter description of backend_api

Parameter	Type	Description
id	String	Web backend ID
status	Integer	Web backend status
url_domain	String	Backend endpoint
version	String	Web backend version
req_protocol	String	Request protocol
req_method	String	Request method
req_uri	String	Access address
timeout	Integer	Timeout duration in milliseconds
register_time	Timestamp	Creation time
update_time	Timestamp	Time when the web backend was last modified
remark	String	Description of the web backend
vpc_status	String	Indicates whether to use a VPC channel.
vpc_info	String	VPC channel information

Table 5-79 Parameter description of mock_info

Parameter	Type	Description
id	String	Mock backend ID
status	Integer	Mock backend status
version	String	Version of the Mock backend
result_content	String	Mock response
register_time	Timestamp	Creation time
update_time	Timestamp	Time when the Mock backend was last modified
remark	String	Description of the Mock backend

Table 5-80 Parameter description of func_info

Parameter	Type	Description
id	String	Function ID
status	Integer	Function status
version	String	Function version
function_urn	String	Function URN
invocation_type	String	Invocation mode, which can be async or sync
register_time	Timestamp	Creation time
update_time	Timestamp	Time when the function was last updated
timeout	Integer	Timeout duration in milliseconds
remark	String	Description of the function

Table 5-81 Parameter description of req_params

Parameter	Type	Description
id	String	Parameter ID
name	String	Parameter name
type	String	Parameter type
location	String	Parameter location
default_value	String	Default value
sample_value	String	Example value
required	Integer	Indicates whether the parameter is mandatory.
valid_enable	Integer	Indicates whether validity check is enabled.
remark	String	Description of the parameter
enumerations	String	Enumerated value
min_num	Integer	Minimum value, which is valid when the parameter type is NUMBER
max_num	Integer	Maximum value, which is valid when the parameter type is NUMBER
min_size	Integer	Minimum length
max_size	Integer	Maximum length

Parameter	Type	Description
regular	String	Regular verification rule (currently not supported)
json_schema	String	JSON verification rule (currently not supported)

Table 5-82 Parameter description of backend_params

Parameter	Type	Description
id	String	Parameter ID
req_param_id	String	ID of the request parameter to which the backend parameter is mapped
name	String	Parameter name
location	String	Parameter location
origin	String	Parameter type
value	String	Parameter value
remark	String	Description of the parameter

Table 5-83 Parameter description of policy_https

Parameter	Type	Description
id	String	Backend policy ID
name	String	Backend name
url_domain	String	Endpoint of the policy backend
req_protocol	String	Request protocol
req_method	String	Request method
req_uri	String	Access address
timeout	Integer	Timeout duration in milliseconds
vpc_status	String	Indicates whether to use a VPC channel.
vpc_info	String	VPC channel information
effect_mode	String	Effective mode of the backend policy
conditions	Dictionary	Policy condition list
backend_params	Dictionary	Backend parameter list

Table 5-84 Parameter description of policy_mocks

Parameter	Type	Description
id	String	Backend policy ID
name	String	Backend name
result_content	String	Mock response
effect_mode	String	Effective mode of the backend policy
conditions	Dictionary	Policy condition list
backend_params	Dictionary	Backend parameter list

Table 5-85 Parameter description of policy_functions

Parameter	Type	Description
id	String	Backend policy ID
name	String	Backend name
version	String	Function version
function_urn	String	Function URN
invocation_type	String	Invocation mode, which can be async or sync
timeout	Integer	Timeout duration in milliseconds
effect_mode	String	Effective mode of the backend policy
conditions	Dictionary	Policy condition list
backend_params	Dictionary	Backend parameter list

Table 5-86 Parameter description of conditions

Parameter	Type	Description
id	String	Backend policy condition ID
condition_type	String	Condition type
condition_value	String	Condition value

Parameter	Type	Description
condition_origin	String	Condition source
req_param_name	String	Input parameter name
req_param_id	String	Input parameter ID
req_param_location	String	Input parameter location

Table 5-87 Parameter description of auth_opt

Parameter	Type	Description
app_code_auth_type	String	Indicates whether AppCode authentication is enabled.

Example response:

```
{
  "name": "test",
  "type": 1,
  "version": "V0.0.1",
  "req_protocol": "HTTPS",
  "req_method": "GET",
  "req_uri": "/test/{tenant_id}",
  "auth_type": "APP",
  "auth_opt": {
    "app_code_auth_type": "DISABLE"
  },
  "tags": ["APIG-SN-test", "test"],
  "cors": false,
  "match_mode": "NORMAL",
  "backend_type": "HTTP",
  "group_id": "f71f69876f90456ca6fd18ed012fdc11",
  "result_normal_sample": "hello world!",
  "id": "81efcfd94b8747a0b21e8c04144a4e8c",
  "status": 1,
  "arrange_necessary": 2,
  "register_time": "2018-08-15T03:41:11.0239936Z",
  "update_time": "2018-08-15T03:41:11.0239936Z",
  "group_name": "group0002",
  "backend_api": {
    "url_domain": "xxxxxxxxxx",
    "req_protocol": "HTTP",
    "req_method": "GET",
    "req_uri": "/test",
    "timeout": 1000,
    "vpc_status": 2,
    "id": "3442ffd031814e3a8f133a9f1ea08453",
    "status": 1,
    "register_time": "2018-08-15T03:41:11.1019236Z",
    "update_time": "2018-08-15T03:41:11.1019236Z"
  },
  "req_params": [
    {
      "name": "tenant_id",
```

```
    "type": "STRING",
    "location": "PATH",
    "required": 1,
    "valid_enable": 2,
    "id": "593c5560e0924e00af08fb458f850ecb"
  },
  {
    "name": "city",
    "type": "STRING",
    "location": "QUERY",
    "required": 2,
    "valid_enable": 2,
    "id": "e0b91bc81ae54f8ea850848d782d6e1e"
  }
],
"backend_params": [
  {
    "name": "tenant_id",
    "location": "QUERY",
    "origin": "REQUEST",
    "value": "tenant_id",
    "id": "44e03de2351e43a8b18ba9ec1e71d2e9",
    "req_param_id": "593c5560e0924e00af08fb458f850ecb"
  },
  {
    "name": "city",
    "location": "QUERY",
    "origin": "REQUEST",
    "value": "city",
    "id": "b60fbc5b86f4f5c8705c445b9bd6325",
    "req_param_id": "e0b91bc81ae54f8ea850848d782d6e1e"
  }
],
"policy_https": [{
  "conditions": [{
    "id": "44e03de2351e43a8b18ba9ec1e71d2e9",
    "condition_type": "pattern",
    "condition_value": "^[0-9]$",
    "condition_origin": "param",
    "req_param_name": "project_id",
    "req_param_id": "b60fbc5b86f4f5c8705c445b9sda325",
    "req_param_location": "PATH"
  }],
  "backend_params": [{
    "name": "project_id",
    "value": "bbbb",
    "location": "QUERY",
    "origin": "REQUEST",
    "id": "44e03de2351e43a8b18ba9ec1e71d2e8",
    "req_param_id": "593c5560e0924e00af08fb458f850ecb"
  }],
  "effect_mode": "ANY",
  "id": "44e03de2351e43a8b18ba9ec1e71d2e8",
  "name": "policy001",
  "req_method": "GET",
  "req_protocol": "http",
  "req_uri": "/test/policy",
  "timeout": 10000,
  "url_domain": "xxxxxxxxxx",
  "vpc_status": 2
}]
}
```

Status Codes

Table 5-88 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
409	Conflict
500	Server Internal Error

5.2.4 Deleting an API

Function

This API is used to delete an API.

This operation will delete all related resources and binding relationships of the API, such as publication records, backend services, and app authorization information.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-89 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/apis/{id}

The following table lists the parameter in the URI.

Table 5-90 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	API ID

Request

N/A

Response

N/A

Status Codes

Table 5-91 Status codes

Status Code	Description
204	No Content
401	Unauthorized
403	Forbidden
404	Not Found
409	Conflict
500	Server Internal Error

5.2.5 Publishing an API

Function

This API is used to publish an API in a specified environment. An API can be called in an environment only after it is published in it. APIs that have not been published cannot be called.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-92 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/apis/publish/{api_id}

The following table lists the parameter in the URI.

Table 5-93 Parameter description

Parameter	Mandatory	Type	Description
api_id	Yes	String	API ID

Request

Table 5-94 Parameter description

Parameter	Mandatory	Type	Description
env_id	Yes	String	ID of the environment in which the API will be published
remark	No	String	Description about the publication The description cannot exceed 255 characters.

Example request:

```
{
  "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "remark": "Published in the production environment"
}
```

Response

Table 5-95 Parameter description

Parameter	Type	Description
publish_id	String	ID of the publication record
api_id	String	API ID
env_id	String	ID of the environment in which the API has been published
remark	String	Description about the publication
publish_time	Timestamp	Time when the API is published
version_id	String	API version

Example response:

```
{
  "publish_id": "5b729aa252764739be2c37ef0d66dc63",
  "api_id": "7addcd00cfab433984b1d8bf2fe08aaa",
  "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
}
```

```
"version_id": "3d9dcb733ba34352b0d02f85fd16b026",  
"remark": "string",  
"publish_time": "2018-07-26T13:18:04.1079916Z"  
}
```

Status Codes

Table 5-96 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.2.6 Taking an API Offline

Function

This API is used to remove an API from an environment in which it has been published. After this operation, the API can no longer be called in the environment.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-97 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/apis/publish/{api_id}[?env_id]

The following table lists the parameters in the URI.

Table 5-98 Parameter description

Parameter	Mandatory	Type	Description
api_id	Yes	String	API ID

Parameter	Mandatory	Type	Description
env_id	Yes	String	ID of the environment in which the API has been published

Request

N/A

Response

N/A

Status Codes

Table 5-99 Status codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
409	Conflict
500	Server Internal Error

5.2.7 Publishing Multiple APIs or Taking Multiple APIs Offline

Function

This API is used to publish multiple APIs in an environment or to remove multiple APIs from the environment in which they have been published.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-100 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/apis/publish[?action]

The following table lists the parameter in the URI.

Table 5-101 Parameter description

Parameter	Mandatory	Type	Description
action	No	String	online: publish offline: take offline

Request

Table 5-102 Parameter description

Parameter	Mandatory	Type	Description
apis	Yes	String Array	IDs of the APIs to be published or taken offline
env_id	Yes	String	Environment ID
remark	No	String	Description of the publication The description cannot exceed 255 characters.

Example request:

```
{
  "apis": ["81efcd94b8747a0b21e8c04144a4e8c", "7addcd00cfab433984b1d8bf2fe08aaa"],
  "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "remark": "Published in the production environment"
}
```

Response

Table 5-103 Parameter description

Parameter	Type	Description
success	Array	Message for successful API publication or taking offline

Parameter	Type	Description
failure	Array	Error message and APIs that fail to be published or taken offline

Table 5-104 Parameter description of success (batch publishing)

Parameter	Type	Description
publish_id	String	Publication record ID
api_id	String	ID of a successfully published API
api_name	String	Name of the API
env_id	String	ID of the environment in which the API has been published
remark	String	Description of the publication
publish_time	Timestamp	Time when the API is published
version_id	String	API version

Table 5-105 Parameter description of success (taking offline in batches)

Parameter	Type	Description
api_id	String	ID of an API that is successfully taken offline
api_name	String	Name of the API

Table 5-106 Parameter description of failure

Parameter	Type	Description
api_id	String	ID of an API that fails to be published or taken offline
api_name	String	Name of the API
error_code	String	Error code
error_msg	String	Error message

Example response:

```
{
  "success": [{
    "publish_id": "5b729aa252764739be2c37ef0d66dc63",
    "api_id": "7addcd00cfab433984b1d8bf2fe08aaa",
```

```
{
  "api_name": "testApi",
  "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "version_id": "3d9dcb733ba34352b0d02f85fd16b026",
  "remark": "string",
  "publish_time": "2018-07-26T13:18:04.1079916Z"
},
"failure": [{
  "api_id": "81efcfd94b8747a0b21e8c04144a4e8c",
  "error_code": "APIG.3002",
  "error_msg": "api with id 81efcfd94b8747a0b21e8c04144a4e8c not found"
}]
}
```

Status Codes

Table 5-107 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.2.8 Querying API Details

Function

This API is used to query the details of a specified API.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-108 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/apis/{id}

The following table lists the parameters in the URI.

Table 5-109 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	API ID

Request

N/A

Response

Table 5-110 Parameter description

Parameter	Type	Description
id	String	API ID
name	String	API name
group_id	String	ID of the API group to which the API belongs
group_name	String	Name of the API group to which the API belongs
status	Integer	API status
type	Integer	API type
version	String	API version
req_protocol	String	Request protocol
req_method	String	Request method
req_uri	String	Access address
auth_type	String	Security authentication mode
auth_opt	Object	Security authentication mode parameter
authorizer_id	String	ID of the frontend custom authorizer
match_mode	String	Matching mode
register_time	Timestamp	Time when the API was created
update_time	Timestamp	Time when the API was last modified
remark	String	API description
backend_type	String	Backend type
run_env_name	String	Name of the environment in which the API has been published

Parameter	Type	Description
run_env_id	String	ID of the environment in which the API has been published
publish_id	String	ID of the publication record
arrange_necessary	Integer	Indicates whether orchestration is required.
tag	String	Service name tag, which is to be discarded
tags	[]String	API tags
cors	Bool	Indicates whether CORS is supported.
body_remark	String	Description of the API request body, which can be an example request body, media type, or parameter information
result_normal_sample	String	Example response for a successful request
result_failure_sample	String	Example response for a failed request
response_id	String	ID of the gateway response
backend_api	Dictionary	Web backend details
mock_info	Dictionary	Mock backend details
func_info	Dictionary	FunctionGraph backend details
req_params	Dictionary	Request parameter list
backend_params	Dictionary	Backend parameter list
policy_https	Dictionary	Web backend policy list
policy_mocks	Dictionary	Mock backend policy list
policy_functions	Dictionary	FunctionGraph backend policy list

Table 5-111 Parameter description of backend_api

Parameter	Type	Description
id	String	Web backend ID
status	Integer	Web backend status
url_domain	String	Backend endpoint
version	String	Web backend version

Parameter	Type	Description
req_protocol	String	Request protocol
req_method	String	Request method
req_uri	String	Access address
timeout	Integer	Timeout duration in milliseconds
register_time	Timestamp	Creation time
update_time	Timestamp	Time when the web backend was last modified
remark	String	Description of the web backend
vpc_status	String	Indicates whether to use a VPC channel.
vpc_info	String	VPC channel information
authorizer_id	String	ID of the backend custom authorizer

Table 5-112 Parameter description of mock_info

Parameter	Type	Description
id	String	Mock backend ID
status	Integer	Mock backend status
version	String	Mock backend version
result_content	String	Mock response
register_time	Timestamp	Creation time
update_time	Timestamp	Time when the Mock backend was last modified
remark	String	Description of the Mock backend

Table 5-113 Parameter description of func_info

Parameter	Type	Description
id	String	Function ID
status	Integer	Function status
version	String	Function version
function_urn	String	Function URN
invocation_type	String	Invocation mode, which can be async or sync

Parameter	Type	Description
register_time	Timestamp	Creation time
update_time	Timestamp	Time when the function was last updated
timeout	Integer	Timeout duration in milliseconds
remark	String	Description of the function

Table 5-114 Parameter description of req_params

Parameter	Type	Description
id	String	Parameter ID
name	String	Parameter name
type	String	Parameter type
location	String	Parameter location
default_value	String	Default value
sample_value	String	Example value
required	Integer	Indicates whether the parameter is mandatory. The value can be: • 1: yes • 2: no
valid_enable	Integer	Indicates whether validity check is enabled.
remark	String	Description of the parameter
enumerations	String	Enumerated value
min_num	Integer	Minimum value, which is valid when the parameter type is NUMBER
max_num	Integer	Maximum value, which is valid when the parameter type is NUMBER
min_size	Integer	Minimum length
max_size	Integer	Maximum length
regular	String	Regular verification rule (currently not supported)
json_schema	String	JSON verification rule (currently not supported)

Table 5-115 Parameter description of backend_params

Parameter	Type	Description
id	String	Parameter ID
req_param_id	String	ID of the request parameter to which the backend parameter is mapped
name	String	Parameter name
location	String	Parameter location
origin	String	Parameter type
value	String	Parameter value
remark	String	Description of the parameter

Table 5-116 Parameter description of policy_https

Parameter	Type	Description
id	String	Backend policy ID
name	String	Backend name
url_domain	String	Endpoint of the policy backend
req_protocol	String	Request protocol
req_method	String	Request method
req_uri	String	Access address
timeout	Integer	Timeout duration in milliseconds
vpc_status	String	Indicates whether to use a VPC channel.
vpc_info	String	VPC channel information
effect_mode	String	Effective mode of the backend policy
conditions	Dictionary	Policy condition list
backend_params	Dictionary	Backend parameter list

Table 5-117 Parameter description of policy_mocks

Parameter	Type	Description
id	String	Backend policy ID
name	String	Backend name

Parameter	Type	Description
result_content	String	Mock response
effect_mode	String	Effective mode of the backend policy
conditions	Dictionary	Policy condition list
backend_params	Dictionary	Backend parameter list

Table 5-118 Parameter description of policy_functions

Parameter	Type	Description
id	String	Backend policy ID
name	String	Backend name
version	String	Function version
function_urn	String	Function URN
invocation_type	String	Invocation mode, which can be async or sync
timeout	Integer	Timeout duration in milliseconds
effect_mode	String	Effective mode of the backend policy
conditions	Dictionary	Policy condition list
backend_params	Dictionary	Backend parameter list

Table 5-119 Parameter description of conditions

Parameter	Type	Description
id	String	Backend policy condition ID
condition_type	String	Condition type
condition_value	String	Condition value
condition_origin	String	Condition source
req_param_name	String	Input parameter name
req_param_id	String	Input parameter ID

Parameter	Type	Description
req_param_location	String	Input parameter location

Table 5-120 Parameter description of auth_opt

Parameter	Type	Description
app_code_auth_type	String	Indicates whether AppCode authentication is enabled.

Example response:

```
{
  "name": "test",
  "type": 1,
  "version": "V0.0.1",
  "req_protocol": "HTTPS",
  "req_method": "GET",
  "req_uri": "/test/{tenant_id}",
  "auth_type": "APP",
  "auth_opt": {
    "app_code_auth_type": "DISABLE"
  },
  "tags": ["APIG-SN-test", "test"],
  "cors": false,
  "match_mode": "NORMAL",
  "backend_type": "HTTP",
  "group_id": "f71f69876f90456ca6fd18ed012fdc11",
  "result_normal_sample": "hello world!",
  "id": "81efcfd94b8747a0b21e8c04144a4e8c",
  "status": 1,
  "arrange_necessary": 2,
  "register_time": "2018-08-15T03:41:11.0239936Z",
  "update_time": "2018-08-15T03:41:11.0239936Z",
  "group_name": "group0002",
  "backend_api": {
    "url_domain": "xxxxxxxxxx",
    "req_protocol": "HTTP",
    "req_method": "GET",
    "req_uri": "/test",
    "timeout": 1000,
    "vpc_status": 2,
    "id": "3442ffd031814e3a8f133a9f1ea08453",
    "status": 1,
    "register_time": "2018-08-15T03:41:11.1019236Z",
    "update_time": "2018-08-15T03:41:11.1019236Z"
  },
  "req_params": [
    {
      "name": "tenant_id",
      "type": "STRING",
      "location": "PATH",
      "required": 1,
      "valid_enable": 2,
      "id": "593c5560e0924e00af08fb458f850ecb"
    },
    {
      "name": "city",
      "type": "STRING",

```

```
    "location": "QUERY",
    "required": 2,
    "valid_enable": 2,
    "id": "e0b91bc81ae54f8ea850848d782d6e1e"
  }
],
"backend_params": [
  {
    "name": "tenant_id",
    "location": "QUERY",
    "origin": "REQUEST",
    "value": "tenant_id",
    "id": "44e03de2351e43a8b18ba9ec1e71d2e9",
    "req_param_id": "593c5560e0924e00af08fb458f850ecb"
  },
  {
    "name": "city",
    "location": "QUERY",
    "origin": "REQUEST",
    "value": "city",
    "id": "b60fbc5b86f4f5c8705c445b9bd6325",
    "req_param_id": "e0b91bc81ae54f8ea850848d782d6e1e"
  }
],
"policy_https": [{
  "conditions": [{
    "id": "44e03de2351e43a8b18ba9ec1e71d2e9",
    "condition_type": "pattern",
    "condition_value": "^[0-9]$",
    "condition_origin": "param",
    "req_param_name": "project_id",
    "req_param_id": "b60fbc5b86f4f5c8705c445b9sda325",
    "req_param_location": "PATH"
  }],
  "backend_params": [{
    "name": "project_id",
    "value": "bbbb",
    "location": "QUERY",
    "origin": "REQUEST",
    "id": "44e03de2351e43a8b18ba9ec1e71d2e8",
    "req_param_id": "593c5560e0924e00af08fb458f850ecb"
  }],
  "effect_mode": "ANY",
  "id": "44e03de2351e43a8b18ba9ec1e71d2e8",
  "name": "policy001",
  "req_method": "GET",
  "req_protocol": "http",
  "req_uri": "/test/policy",
  "timeout": 10000,
  "url_domain": "xxxxxxxxxx",
  "vpc_status": 2
}]
}
```

Status Codes

Table 5-121 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized

Status Code	Description
403	Forbidden
404	Not Found

5.2.9 Querying an API List

Function

This API is used to query an API list to return details and publication information of the APIs. Backend information of the APIs will not be returned.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-122 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/apis[?page_size, page_no, id, name, group_id, req_protocol, req_method, req_uri, auth_type, env_id, type,status, tags]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **ID, name, group_id, req_protocol, req_method, req_uri, auth_type, env_id, type, status, tags, page_size**, and **page_no**.

Request

Table 5-123 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	API ID
name	No	String	API name
group_id	No	String	ID of the API group to which the API belongs
req_protocol	No	String	Request protocol
req_method	No	String	Request method
req_uri	No	String	Request path

Parameter	Mandatory	Type	Description
auth_type	No	String	Security authentication mode
env_id	No	String	ID of the environment in which the API has been published
type	No	Integer	API type
page_size	No	Integer	Number of records displayed on each page. The default value is 20 and the maximum value is 500 . When the value of page_size is set to 0 , all APIs are returned.
page_no	No	Integer	Page number. The default value is 1 .
precise_search	No	String	Parameter name (name or req_uri) for exact matching

Response

Table 5-124 Parameter description

Parameter	Type	Description
total	Integer	Number of APIs that match the query conditions
size	Integer	Length of the returned API list
apis	Dictionary	API list

Table 5-125 Parameter description of apis

Parameter	Type	Description
id	String	API ID
name	String	API name
group_id	String	ID of the API group to which the API belongs
group_name	String	Name of the API group to which the API belongs
status	Integer	API status
type	Integer	API type
version	String	API version

Parameter	Type	Description
req_protocol	String	Request protocol
req_method	String	Request method
req_uri	String	Access address
auth_type	String	Security authentication mode
auth_opt	Object	Security authentication mode parameter
authorizer_id	String	ID of the frontend custom authorizer
match_mode	String	Matching mode
register_time	Timestamp	Time when the API was created
update_time	Timestamp	Time when the API was last modified
remark	String	API description
bakend_type	String	Backend type
run_env_name	String	Name of the environment in which the API has been published
run_env_id	String	ID of the environment in which the API has been published
publish_id	String	ID of the publication record
arrange_necessary	Integer	Indicates whether orchestration is required.
cors	Bool	Indicates whether CORS is supported.
tag	String	Service name tag, which is to be discarded
tags	[]String	API tags
response_id	String	ID of the gateway response

Table 5-126 Parameter description of auth_opt

Parameter	Type	Description
app_code_auth_type	String	Indicates whether AppCode authentication is enabled.

Example response:

```
{
  "total": 3,
  "size": 3,
  "apis": [
    {
```

```
"name": "test",
"type": 1,
"version": "V0.0.1",
"req_protocol": "HTTPS",
"req_method": "GET",
"req_uri": "/test/{project_id}",
"auth_type": "APP",
"auth_opt": {
  "app_code_auth_type": "DISABLE"
},
"tags": ["APIG-SN-test", "test"],
"cors": false,
"match_mode": "NORMAL",
"backend_type": "HTTP",
"group_id": "f71f69876f90456ca6fd18ed012fdc11",
"id": "81efcfd94b8747a0b21e8c04144a4e8c",
"status": 1,
"arrange_necessary": 2,
"register_time": "2018-08-15T03:41:11Z",
"update_time": "2018-08-15T03:41:11Z",
"group_name": "group0002"
},
{
  "name": "bbbb",
  "type": 1,
  "version": "0.0.1",
  "req_protocol": "HTTPS",
  "req_method": "GET",
  "req_uri": "/test002",
  "auth_type": "APP",
  "auth_opt": {
    "app_code_auth_type": "DISABLE"
  },
  "tags": ["APIG-SN-test", "test"],
  "cors": false,
  "match_mode": "NORMAL",
  "backend_type": "MOCK",
  "remark": "aaa",
  "group_id": "70f1b578da9b4dfe889b4c33d1b995c2",
  "id": "91c26288acea4448be205265d77dae22",
  "status": 1,
  "arrange_necessary": 2,
  "register_time": "2018-07-27T11:54:24Z",
  "update_time": "2018-07-27T11:54:24Z",
  "group_name": "test001",
  "run_env_name": "RELEASE",
  "run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "publish_id": "a6e06a00c382436eb524fa2dd343cb6d"
},
{
  "name": "aaa",
  "type": 1,
  "version": "0.0.1",
  "req_protocol": "HTTPS",
  "req_method": "GET",
  "req_uri": "/test001",
  "auth_type": "APP",
  "auth_opt": {
    "app_code_auth_type": "DISABLE"
  },
  "tags": ["APIG-SN-test", "test"],
  "cors": false,
  "match_mode": "NORMAL",
  "backend_type": "MOCK",
  "remark": "aaa",
  "group_id": "70f1b578da9b4dfe889b4c33d1b995c2",
  "id": "aebacac6095942b4b2dd2b209bb7b9bc",
  "status": 1,
  "arrange_necessary": 2,
```

```
"register_time": "2018-07-27T11:23:34Z",
"update_time": "2018-07-27T11:23:34Z",
"group_name": "test001",
"run_env_name": "RELEASE",
"run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
"publish_id": "1bc8b2b741a04bd4af3ef9d7cd003104"
}
]
}
```

Status Codes

Table 5-127 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
500	Server Internal Error

5.2.10 Querying Historical API Versions

Function

This API is used to query the historical versions of an API. APIG retains a maximum of 10 historical versions for each API in an environment.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-128 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/apis/publish/{api_id}[?env_id,env_name]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **env_id** and **env_name**.

The following table lists the parameters in the URI.

Table 5-129 Parameter description

Parameter	Mandatory	Type	Description
api_id	Yes	String	API ID
env_id	No	String	ID of the environment in which the API has been published
env_name	No	String	Name of the environment in which the API has been published

Request

N/A

Response

Table 5-130 Parameter description

Parameter	Type	Description
total	Integer	Number of historical versions that match the query conditions
size	Integer	Length of the returned historical version list
api_versions	Dictionary	Historical version list

Table 5-131 Parameter description of api_versions

Parameter	Type	Description
version_id	String	API version ID
version_no	String	API version
api_id	String	API ID
env_id	String	ID of the environment in which the API has been published
env_name	String	Name of the environment in which the API has been published
remark	String	Description about the publication
publish_time	Timestamp	Time when the API is published

Parameter	Type	Description
status	Integer	Version status, which can be: • Effective • Not effective

Example response:

```
{
  "total": 1,
  "size": 1,
  "api_versions": [
    {
      "version_id": "04c194dc7b5340ed942f2451702060da",
      "version_no": "20180722102526",
      "api_id": "acf141aa6279415088b593a4bbb55eed",
      "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
      "env_name": "RELEASE",
      "publish_time": "2018-04-14T07:32:23Z",
      "status": 2
    }
  ]
}
```

Status Codes

Table 5-132 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.2.11 Taking an Effective Version of an API Offline

Function

This API is used to remove an effective version of an API. After this operation, the API cannot be called in the environment in which it takes effect.

This API is provided for FunctionGraph.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-133 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/apis/versions/{version_id}

The following table lists the parameter in the URI.

Table 5-134 Parameter description

Parameter	Mandatory	Type	Description
version_id	Yes	String	API version ID

Request

N/A

Response

N/A

Status Codes

Table 5-135 Status codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.2.12 Querying Details of an API Version

Function

This API is used to query the details of a specified API version.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-136 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/apis/versions/{version_id}

The following table lists the parameter in the URI.

Table 5-137 Parameter description

Parameter	Mandatory	Type	Description
version_id	Yes	String	API version ID

Request

N/A

Response

Table 5-138 Parameter description

Parameter	Type	Description
id	String	API ID
name	String	API name
group_id	String	ID of the API group to which the API belongs
group_name	String	Name of the API group to which the API belongs
status	Integer	API status
type	Integer	API type
version	String	API version
req_protocol	String	Request protocol
req_method	String	Request method
req_uri	String	Access address
auth_type	String	Security authentication mode
auth_opt	Object	Security authentication mode parameter
authorizer_id	String	ID of the frontend custom authorizer
match_mode	String	Matching mode

Parameter	Type	Description
register_time	Timestamp	Time when the API was created
update_time	Timestamp	Time when the API was last modified
remark	String	Description of the API
backend_type	String	Backend type
run_env_name	String	Name of the environment in which the API has been published
run_env_id	String	ID of the environment in which the API has been published
publish_id	String	ID of the publication record
arrange_necessary	Integer	Indicates whether orchestration is required.
tag	String	Service name tag, which is to be discarded
tags	[]String	API tags
cors	Bool	Indicates whether CORS is supported.
body_remark	String	Description of the API request body, which can be an example request body, media type, or parameter information
result_normal_sample	String	Example response for a successful request
result_failure_sample	String	Example response for a failed request
response_id	String	ID of the gateway response
sl_domain	String	Subdomain name of the API group
sl_domains	Array of strings	List of subdomain names bound to the API group
version_id	String	API version
publish_time	Timestamp	Time when the API version is published
backend_api	Dictionary	Web backend details
mock_info	Dictionary	Mock backend details
func_info	Dictionary	FunctionGraph backend details
req_params	Dictionary	Request parameter list
backend_params	Dictionary	Backend parameter list

Table 5-139 Parameter description of backend_api

Parameter	Type	Description
id	String	Web backend ID
status	Integer	Web backend status
url_domain	String	Backend endpoint
version	String	Backend version
req_protocol	String	Request protocol
req_method	String	Request method
req_uri	String	Access address
timeout	Integer	Timeout duration in milliseconds
register_time	Timestamp	Creation time
update_time	Timestamp	Time when the web backend was last modified
remark	String	Description of the backend
vpc_status	String	Indicates whether to use a VPC channel.
vpc_info	String	VPC channel information
authorizer_id	String	ID of the backend custom authorizer

Table 5-140 Parameter description of mock_info

Parameter	Type	Description
id	String	Mock backend ID
status	Integer	Mock backend status
version	String	Backend version
result_content	String	Mock response
register_time	Timestamp	Creation time
update_time	Timestamp	Time when the Mock backend was last modified
remark	String	Description of the backend

Table 5-141 Parameter description of func_info

Parameter	Type	Description
id	String	Function ID

Parameter	Type	Description
status	Integer	Function status
version	String	Function version
function_urn	String	Function URN
invocation_type	String	Invocation mode, which can be async or sync
register_time	Timestamp	Creation time
update_time	Timestamp	Time when the function was last updated
timeout	Integer	Timeout duration in milliseconds
remark	String	Description of the function

Table 5-142 Parameter description of req_params

Parameter	Type	Description
id	String	Parameter ID
name	String	Parameter name
type	String	Parameter type
location	String	Parameter location
default_value	String	Default value
sample_value	String	Example value
required	Integer	Indicates whether the parameter is mandatory.
valid_enable	Integer	Indicates whether validity check is enabled.
remark	String	Description of the parameter
enumerations	String	Enumerated value
min_num	Integer	Minimum value, which is valid when the parameter type is NUMBER
max_num	Integer	Maximum value, which is valid when the parameter type is NUMBER
min_size	Integer	Minimum length
max_size	Integer	Maximum length
regular	String	Regular expression validation rule
json_schema	String	JSON validation rule

Table 5-143 Parameter description of backend_params

Parameter	Type	Description
id	String	Parameter ID
req_param_id	String	ID of the request parameter to which the backend parameter is mapped
name	String	Parameter name
location	String	Parameter location
origin	Integer	Parameter type
value	Integer	Parameter value
remark	String	Description of the parameter

Table 5-144 Parameter description of auth_opt

Parameter	Type	Description
app_code_auth_type	String	Indicates whether AppCode authentication is enabled.

Example response:

```
{
  "name": "test",
  "type": 1,
  "version": "V0.0.1",
  "req_protocol": "HTTPS",
  "req_method": "GET",
  "req_uri": "/test/{project_id}",
  "auth_type": "APP",
  "auth_opt": {
    "app_code_auth_type": "HEADER"
  },
  "tags": ["APIG-SN-test", "test"],
  "cors": false,
  "match_mode": "NORMAL",
  "backend_type": "HTTP",
  "group_id": "f71f69876f90456ca6fd18ed012fdc11",
  "result_normal_sample": "hello world!",
  "id": "81efcd94b8747a0b21e8c04144a4e8c",
  "status": 1,
  "arrange_necessary": 2,
  "register_time": "2018-08-15T03:41:11.0239936Z",
  "update_time": "2018-08-15T03:41:11.0239936Z",
  "group_name": "group0002",
  "sl_domain": "a8be0e466f0e4d8bb18ebd15402cdd66.apigw.example.com",
  "sl_domains": ["a8be0e466f0e4d8bb18ebd15402cdd66.apigw.example.com",
    "a8be0e466f0e4d8bb18ebd15402cdd66.apigw.example.cn"],
  "version_id": "69b7492e2855487398d45733b9d6147a",
  "publish_time": "2018-08-24T03:10:14Z",
  "backend_api": {
    "url_domain": "xxxxxxxxx",
    "req_protocol": "HTTP",
    "req_method": "GET",
  }
}
```

```
{
  "req_uri": "/test",
  "timeout": 1000,
  "vpc_status": 2,
  "id": "3442ffd031814e3a8f133a9f1ea08453",
  "status": 1,
  "register_time": "2018-08-15T03:41:11.1019236Z",
  "update_time": "2018-08-15T03:41:11.1019236Z"
},
"req_params": [
  {
    "name": "project_id",
    "type": "STRING",
    "location": "PATH",
    "required": 1,
    "valid_enable": 2,
    "id": "593c5560e0924e00af08fb458f850ecb"
  },
  {
    "name": "city",
    "type": "STRING",
    "location": "QUERY",
    "required": 2,
    "valid_enable": 2,
    "id": "e0b91bc81ae54f8ea850848d782d6e1e"
  }
],
"backend_params": [
  {
    "name": "project_id",
    "location": "QUERY",
    "origin": "REQUEST",
    "value": "project_id",
    "id": "44e03de2351e43a8b18ba9ec1e71d2e9",
    "req_param_id": "593c5560e0924e00af08fb458f850ecb"
  },
  {
    "name": "city",
    "location": "QUERY",
    "origin": "REQUEST",
    "value": "city",
    "id": "b60fbc5b86f4f5c8705c445b9bd6325",
    "req_param_id": "e0b91bc81ae54f8ea850848d782d6e1e"
  }
]
}
```

Status Codes

Table 5-145 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.2.13 Querying the Runtime Definition of an API

Function

This API is used to query the runtime definition of an API in a specified environment. The runtime definition of an API in the RELEASE environment is queried if no environment is specified.

The definition of an API is classified into the following types:

- Temporary definition: definition of an API used after the API was last edited.
- Runtime definition: snapshot of the temporary definition of an API captured when the API is published in an environment.

The runtime definition of an API is accessed when the API is called in an environment.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-146 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/apis/runtime/{id}[?env_id]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- The query condition is **env_id**.

The following table lists the parameter in the URI.

Table 5-147 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	API ID

Request

Table 5-148 Parameter description

Parameter	Mandatory	Type	Description
env_id	No	String	ID of the environment in which the API is published

Response

Table 5-149 Parameter description

Parameter	Type	Description
id	String	API ID
name	String	API name
group_id	String	ID of the API group to which the API belongs
group_name	String	Name of the API group to which the API belongs
type	Integer	API type
version	String	API version
req_protocol	String	Request protocol
req_method	String	Request method
req_uri	String	Access address
auth_type	String	Security authentication mode
auth_opt	Object	Security authentication mode parameter
authorizer_id	String	ID of the frontend custom authorizer
match_mode	String	Matching mode
remark	String	Description of the API
backend_type	String	Backend type
run_env_name	String	Name of the environment in which the API has been published
run_env_id	String	ID of the environment in which the API has been published
publish_id	String	ID of the publication record

Parameter	Type	Description
tag	String	Service name tag, which is to be discarded
tags	[]String	API tags
cors	Bool	Indicates whether CORS is supported.
body_remark	String	Description of the API request body, which can be an example request body, media type, or parameter information
result_normal_sample	String	Example response for a successful request
result_failure_sample	String	Example response for a failed request
response_id	String	ID of the gateway response
sl_domain	String	Subdomain name of the API group
sl_domains	Array of strings	List of subdomain names bound to the API group
req_params	Dictionary	Request parameter list

Table 5-150 Parameter description of req_params

Parameter	Type	Description
id	String	Parameter ID
name	String	Parameter name
type	String	Parameter type
location	String	Parameter location
default_value	String	Default value
sample_value	String	Example value
required	Integer	Indicates whether the parameter is mandatory.
valid_enable	Integer	Indicates whether validity check is enabled.
remark	String	Description of the parameter
enumerations	String	Enumerated value
min_num	Integer	Minimum value, which is valid when the parameter type is NUMBER
max_num	Integer	Maximum value, which is valid when the parameter type is NUMBER

Parameter	Type	Description
min_size	Integer	Minimum length
max_size	Integer	Maximum length
regular	String	Regular expression validation rule
json_schema	String	JSON validation rule

Table 5-151 Parameter description of auth_opt

Parameter	Type	Description
app_code_auth_type	String	Indicates whether AppCode authentication is enabled.

Example response:

```
{
  "name": "market_api01",
  "type": 1,
  "version": "V0.0.1",
  "req_protocol": "HTTPS",
  "req_method": "GET",
  "req_uri": "/test01",
  "auth_type": "APP",
  "auth_opt": {
    "app_code_auth_type": "HEADER"
  },
  "tags": ["APIG-SN-test", "test"],
  "cors": true,
  "match_mode": "NORMAL",
  "backend_type": "MOCK",
  "remark": "market_api01",
  "group_id": "7f848adc971749cda9c6aff3877cfc3e",
  "body_remark": "market_api01",
  "result_normal_sample": "success",
  "result_failure_sample": "",
  "id": "0e51b689e0784bc884f43756bbf34fa5",
  "group_name": "market_group01",
  "run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "run_env_name": "RELEASE",
  "publish_id": "f07eb9f5e5ba4bbf8e89326f5cae99c7",
  "sl_domain": "61297835ff1e4905b6f635dbcdf1777e.apigw.example.com",
  "sl_domains": ["61297835ff1e4905b6f635dbcdf1777e.apigw.example.com",
    "61297835ff1e4905b6f635dbcdf1777e.apigw.example.cn"],
  "req_params": [
    {
      "name": "project_id",
      "type": "STRING",
      "location": "PATH",
      "default_value": "",
      "sample_value": "",
      "required": 1,
      "valid_enable": 2,
      "remark": "",
      "enumerations": "",
      "min_num": 0,
      "max_num": 0,
      "min_size": 0,

```

```
"max_size": 0,  
"regular": "",  
"json_schema": "",  
"id": "2a61905ea2304186a9422faba2940735"  
}  
]  
}
```

Status Codes

Table 5-152 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

5.2.14 Debugging an API

Function

This API is used to debug the definition of an API in a specified environment. The API caller must have the permissions required for operating this API.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-153 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/apis/debug/{api_id}

The following table lists the parameter in the URI.

Table 5-154 Parameter description

Parameter	Mandatory	Type	Description
api_id	Yes	String	API ID

Request

Table 5-155 Parameter description

Parameter	Mandatory	Type	Description
scheme	Yes	String	Request protocol, which can be: • HTTP • HTTPS
method	Yes	String	Request method, which can be: • GET • POST • PUT • DELETE • HEAD • PATCH • OPTIONS
domain	No	String	Access domain name of the API. If no value is specified, one of the following default values will be used based on the setting of mode : • For DEVELOPER, the subdomain name of the API group will be used. • For MARKET, the domain name of the API group allocated by KooGallery will be used. • For CONSUMER, the subdomain name of the API group will be used.
path	Yes	String	Request path of the API, starting with a slash (/) and with up to 1024 characters NOTE The request path must meet path requirements so that it can be correctly decoded after percent-encoding.

Parameter	Mandatory	Type	Description
query	No	Dictionary	Query parameters, with each value being a character string array. Each parameter name must meet the following requirements: • Contains letters, digits, periods (.), hyphens (-), or underscores (_). • Starts with a letter, with a maximum length of 32 bytes. • Case-insensitive and not starts with X-Apig- or X-Sdk-. • Case-insensitive and cannot be X-Stage.
header	No	Dictionary	Header parameters, with each value being a character string array. Each parameter name must meet the following requirements: • Contains letters, digits, periods (.), and hyphens (-). • Starts with a letter, with a maximum length of 32 bytes. • Case-insensitive and not starts with X-Apig- or X-Sdk-. • Case-insensitive and cannot be X-Stage. • Case-insensitive and cannot be X-Auth-Token or Authorization when mode is set to MARKET or CONSUMER. NOTE Each header name is normalized before use. For example, x-MY-hEaDer is normalized as X-My-Header.
body	No	String	Message body, with a maximum length of 2,097,152 bytes.

Parameter	Mandatory	Type	Description
mode	Yes	String	Debugging mode, which can be: • DEVELOPER: debugs the definition of an API that has not been published. • MARKET: debugs the definition of an API purchased from KooGallery. • CONSUMER: debugs the definition of an API that has been published in a specified environment. NOTE In DEVELOPER mode, the API caller must be the API owner. In MARKET mode, the API caller must be the API purchaser or owner. In CONSUMER mode, the API caller must be the API owner or has authorized its access to apps in the specified environment.
app_key	No	String	AppKey used in the debugging request
app_secret	No	String	AppSecret used in the debugging request
stage	No	String	Running environment specified in the debugging request. This parameter is valid only when mode is set to CONSUMER . If no value is specified, RELEASE is used.

Example request:

```
{
  "mode": "DEVELOPER",
  "scheme": "HTTPS",
  "method": "GET",
  "path": "/test",
  "query": {
    "city": [
      "city01",
      "city02"
    ]
  },
  "header": {
    "X-My-City": [
      "city01",
      "city02"
    ]
  }
}
```

Response

Table 5-156 Parameter description

Parameter	Type	Description
request	String	Body of the debugging request
response	String	Body of the debugging response, with a maximum length of 2,097,152 bytes. Any content beyond this threshold will be truncated. NOTE Any content beyond the length limit will be truncated, and text [TRUNCATED] will be added to the response body.
latency	String	Debugging duration in milliseconds
log	String	Debugging logs

Example response:

```
{
  "request": "GET /test?city=city01&city=city02 HTTP/1.1\r\nHost:
edf94892b11d440795562cb81c5be059.apigw.example.com\r\nUser-Agent: APIGatewayDebugClient/1.0\r\nX-
Apig-Mode: debug\r\nX-My-City: city01\r\nX-My-City: city02\r\n\r\n",
  "response": "HTTP/1.1 200 OK\r\nContent-Length: 33\r\nConnection: keep-alive\r\nContent-Type:
application/json; charset=utf-8\r\nDate: Fri, 24 Aug 2018 10:36:47 GMT\r\nServer: api-gateway\r\nX-Apig-
Latency: 13\r\nX-Apig-Ratelimit-API: remain:92,limit:100,time:1 minute\r\nX-Apig-Ratelimit-API-Allenv:
remain:9,limit:10,time:1 second\r\nX-Apig-Upstream-Latency: 1\r\nX-Request-Id:
12f69943cc2fa4f8a3674ee947655339\r\n\r\n{\r\n  \"version\": \"4.0.12.201808190004\"
}\r\n",
  "latency": "12",
  "log": ""
}
```

Status Codes

Table 5-157 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

5.3 App Management

5.3.1 Object Model

This section describes the app object model.

 NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of C is mandatory.

Table 5-158 App object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	App ID	R	-
name	String	App name	CRU	Yes
status	Integer	App status, which can be: • 1: enabled • 2: disabled • 3: deleted Default value: 1 This parameter is not used currently.	R	-
appkey	String	AppKey, which is globally unique	R	-
app_secret	String	AppSecret	RU	-
project_id	String	ID of the tenant to which the app belongs, that is, the user that creates the app	-	-
remark	String	Description of the app	CRU	No
register_time	Timestamp	Creation time	R	-
update_time	Timestamp	Time when the app was last updated	R	-

5.3.2 Creating an App

Function

This API is used to create an app. An app is an identity for accessing an API. An app can call the APIs to which it has been authorized.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-159 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/apps

Request

Table 5-160 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	App name An app name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
remark	No	String	Description of the app The description cannot exceed 255 characters.
app_key	No	String	AppKey An AppKey consists of 8–64 characters, starting with a letter or digit. Only letters, digits, underscores (_), and hyphens (-) are allowed. NOTE This parameter is available in some regions.
app_secret	No	String	AppSecret An AppSecret consists of 8–64 characters, starting with a letter or digit. Only letters, digits, and the following special characters are allowed: _!@#\$\$% NOTE This parameter is available in some regions.

Example request:

```
{
  "name": "app_001",
  "remark": "first app",
  "app_key": "app_key_sample",
  "app_secret": "app_secret_sample"
}
```

Response

Table 5-161 Parameter description

Parameter	Type	Description
id	String	App ID
name	String	App name
status	Integer	App status
app_key	String	AppKey
app_secret	String	AppSecret
creator	String	App creator, which can be: ● USER: The app is created by the API user. ● MARKET: The app is allocated by KooGallery.
register_time	Timestamp	Creation time
remark	String	Description of the app
update_time	Timestamp	Time when the app was last updated
app_type	String	App type. The default value is apig .

Example response:

```
{
  "id": "14b3****537e9",
  "name": "app_001",
  "status": 1,
  "app_key": "d49b1****376eb",
  "app_secret": "*****",
  "creator": "USER",
  "remark": "First app",
  "register_time": "2017-12-28T12:26:54.2345858Z",
  "update_time": "2017-12-28T12:26:54.2345858Z",
  "app_type": "apig"
}
```

Status Codes

Table 5-162 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
500	Server Internal Error

5.3.3 Modifying an App

Function

This API is used to modify the information about a specified app. The following parameters can be modified: **name** and **remark**. If the function of customizing keys and secrets is enabled, **app_key** and **app_secret** can also be modified. Other parameters cannot be modified.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-163 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/apps/{id}

The following table lists the parameter in the URI.

Table 5-164 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	App ID, which can be obtained by querying the app list

Request

Table 5-165 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	App name An app name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
remark	No	String	Description of the app The description cannot exceed 255 characters.
app_key	No	String	AppKey An AppKey consists of 8–64 characters, starting with a letter or digit. Only letters, digits, underscores (_), and hyphens (-) are allowed. NOTE This parameter is available in some regions.
app_secret	No	String	AppSecret An AppSecret consists of 8–64 characters, starting with a letter or digit. Only letters, digits, and the following special characters are allowed: _-!@#\$\$% NOTE This parameter is available in some regions.

Example request:

```
{
  "name": "app_001",
  "remark": "First app",
  "app_key": "app_key_sample",
  "app_secret": "app_secret_sample"
}
```

Response

Table 5-166 Parameter description

Parameter	Type	Description
id	String	App ID
name	String	App name
status	Integer	App status

Parameter	Type	Description
app_key	String	AppKey
app_secret	String	AppSecret
creator	String	App creator, which can be: ● USER: The app is created by the API user. ● MARKET: The app is allocated by KooGallery.
register_time	Timestamp	Creation time
remark	String	Description of the app
update_time	Timestamp	Time when the app was last updated
app_type	String	App type. The default value is apig .

Example response:

```
{
  "id": "14b3****37e9",
  "name": "app_001",
  "status": 1,
  "app_key": "d49b1****e376eb",
  "app_secret": "*****",
  "creator": "USER",
  "remark": "First app",
  "register_time": "2017-12-28T12:26:54Z",
  "update_time": "2017-12-28T12:28:07.2966182Z",
  "app_type": "apig"
}
```

Status Codes

Table 5-167 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.3.4 Resetting an AppSecret

Function

This API is used to reset the secret of a specified app.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-168 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/apps/secret/{id}

The following table lists the parameter in the URI.

Table 5-169 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	App ID, which can be obtained by querying the app list

Request

Table 5-170 Parameter description

Parameter	Mandatory	Type	Description
app_secret	No	String	AppSecret An AppSecret consists of 8–64 characters, starting with a letter or digit. Only letters, digits, and the following special characters are allowed: _-!@\$% NOTE This parameter is available in some regions.

Example request:

```
{
  "app_secret": "app_secret_sample"
}
```

Response

Table 5-171 Parameter description

Parameter	Type	Description
id	String	App ID
name	String	App name
status	Integer	App status
app_key	String	AppKey
app_secret	String	AppSecret
creator	String	App creator, which can be: • USER: The app is created by the API user. • MARKET: The app is allocated by KooGallery.
register_time	Timestamp	Creation time
remark	String	Description of the app
update_time	Timestamp	Time when the app was last updated

Example response:

```
{
  "id": "14b399****537e9",
  "name": "app_001",
  "status": 1,
  "app_key": "d49b1cb****8e376eb",
  "app_secret": "*****",
  "creator": "USER",
  "remark": "First app",
  "register_time": "2017-12-28T12:26:54Z",
  "update_time": "2017-12-28T12:29:35.571Z"
}
```

Status Codes

Table 5-172 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

Status Code	Description
500	Server Internal Error

5.3.5 Deleting an App

Function

This API is used to delete an app.

Deleted apps cannot call any APIs. Apps automatically created by KooGallery cannot be deleted.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-173 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/apps/{id}

The following table lists the parameter in the URI.

Table 5-174 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	App ID

Request

N/A

Response

N/A

Status Codes

Table 5-175 Status codes

Status Code	Description
204	No Content

Status Code	Description
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
409	Conflict
500	Server Internal Error

5.3.6 Verifying an App

Function

This API is used to check whether an app exists. This API can be used by people except the app owner to verify an app. Only the basic information, such as **ID**, **name**, and **remark**, of the app is displayed.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-176 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/apps/validation/{id}

The following table lists the parameter in the URI.

Table 5-177 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	App ID

Request

N/A

Response

Table 5-178 Parameter description

Parameter	Type	Description
id	String	App ID
name	String	App name
remark	String	Description of the app

Example response:

```
{
  "id": "14b399ac-967f-4115-bb62-c0346b4537e9",
  "name": "app_001",
  "remark": "First app"
}
```

Status Codes

Table 5-179 Status codes

Status Code	Description
200	OK
401	Unauthorized
404	Not Found
500	Server Internal Error

5.3.7 Querying App Details

Function

This API is used to query the details of a specified app.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-180 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/apps/{id}

The following table lists the parameter in the URI.

Table 5-181 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	App ID

Request

N/A

Response

Table 5-182 Parameter description

Parameter	Type	Description
id	String	App ID
name	String	App name
status	Integer	App status
app_key	String	AppKey
app_secret	String	AppSecret
creator	String	App creator, which can be: • USER: The app is created by the API user. • MARKET: The app is allocated by KooGallery.
register_time	Timestamp	Creation time
remark	String	Description of the app
update_time	Timestamp	Time when the app was last updated
app_type	String	App type. The default value is apig .

Example response:

```
{
  "id": "14b399a****4537e9",
  "name": "app_001",
  "status": 1,
  "app_key": "d49b1****e376eb",
  "app_secret": "*****",
  "creator": "USER",
  "remark": "First app",
  "register_time": "2017-12-28T12:26:54Z",
  "update_time": "2017-12-28T12:28:07.2966182Z",
  "app_type": "apig"
}
```

Status Codes

Table 5-183 Status codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.3.8 Querying an App List

Function

This API is used to query a list of apps that match specified conditions.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-184 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/apps[?page_size, page_no, id, name, app_key, creator]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **id**, **name**, **app_key**, **creator**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-185 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	App ID
name	No	String	App name
status	No	Integer	App status

Parameter	Mandatory	Type	Description
app_key	No	String	AppKey
creator	No	String	App creator, which can be: • USER: The app is created by the API user. • MARKET: The app is allocated by KooGallery.
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .
precise_search	No	String	Parameter name (name) for exact matching

Request

N/A

Response

Table 5-186 Parameter description

Parameter	Type	Description
total	Integer	Number of apps that match the query conditions
size	Integer	Length of the returned app list
apps	Dictionary	App list

Table 5-187 Parameter description of apps

Parameter	Type	Description
id	String	App ID

Parameter	Type	Description
name	String	App name
status	Integer	App status
app_key	String	AppKey
app_secret	String	AppSecret
register_time	Timestamp	Creation time
remark	String	Description of the app
update_time	Timestamp	Time when the app was last updated
creator	String	App creator, which can be: ● USER: The app is created by the API user. ● MARKET: The app is allocated by KooGallery.
app_type	String	App type. The default value is apig .
bind_num	Integer	Number of APIs to which the app has been bound

Example response:

```
{
  "total": 2,
  "size": 2,
  "apps": [{
    "id": "98ef****a286a4",
    "name": "app_002",
    "status": 1,
    "app_key": "f627f****54d3fe2",
    "app_secret": "*****",
    "remark": "Second app",
    "register_time": "2017-12-28T12:32:50Z",
    "update_time": "2017-12-28T12:32:50Z",
    "creator": "MARKET",
    "app_type": "apig",
    "bind_num": 2
  },
  {
    "id": "14b39****4537e9",
    "name": "app_001",
    "status": 1,
    "app_key": "d49b****76eb",
    "app_secret": "*****",
    "remark": "First app",
    "register_time": "2017-12-28T12:26:54Z",
    "update_time": "2017-12-28T12:29:35.571Z",
    "creator": "USER",
    "app_type": "apig",
    "bind_num": 2
  }
]
```

Status Codes

Table 5-188 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
500	Server Internal Error

5.3.9 Creating an AppCode

Function

An AppCode is a sub-module of an app and can be used for simple app authentication. This API is used to create an AppCode.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-189 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/apps/{app_id}/app-codes

The following table lists the parameters in the URI.

Table 5-190 Parameter description

Parameter	Mandatory	Type	Description
app_id	Yes	String	App ID

Request

Table 5-191 Parameter description

Parameter	Mandatory	Type	Description
app_code	Yes	String	App name An app name consists of 64–180 characters, starting with a letter, plus sign (+), or slash (/). Only letters and the following special characters are allowed: +_!@#\$/=

Example request:

```
{
  "app_code": "GjOD3g80AABuuFeEJpVQADBlAjBh3UzC7W
+gr4VJBB5BtJ4fdVOQoSvoji3gFxUDb5pWBz9wUcw9+8/bFZ1B/4pq29wCMQC0pQWX6zTndljDEl99As1pw
+WntAU9xcq+ffagoH6zDpKUvdxV6Ezj8LcCcPZN6BU="
}
```

Response

Table 5-192 Parameter description

Parameter	Type	Description
id	String	AppCode ID
app_code	String	AppCode value
app_id	String	App ID
create_time	Timestamp	Time when the AppCode is created

Example response:

```
{
  "app_code": "GjOD3g80AABuuFeEJpVQADBlAjBh3UzC7W
+gr4VJBB5BtJ4fdVOQoSvoji3gFxUDb5pWBz9wUcw9+8/bFZ1B/4pq29wCMQC0pQWX6zTndljDEl99As1pw
+WntAU9xcq+ffagoH6zDpKUvdxV6Ezj8LcCcPZN6BU=",
  "id": "2fb07c4391d0401696ed345dd1229158",
  "app_id": "db246f3f2ecd45f29ecb0f305e821fdc",
  "create_time": "2019-06-05T04:57:14.470987604Z"
}
```

Status Codes

Table 5-193 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
500	Server Internal Error

5.3.10 Generating an AppCode

Function

This API is used to generate a random AppCode.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-194 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/apps/{app_id}/app-codes

The following table lists the parameters in the URI.

Table 5-195 Parameter description

Parameter	Mandatory	Type	Description
app_id	Yes	String	App ID

Request

N/A

Response

Table 5-196 Parameter description

Parameter	Type	Description
id	String	AppCode ID
app_code	String	AppCode value
app_id	String	App ID
create_time	Timestamp	Time when the AppCode is generated

Example response:

```
{
  "app_code": "GjOD3g80AABuuFeEJpVQADBIAjBh3UzC7W
+gr4VJBB5BtJ4fdVOQoSvoji3gFxUDb5pWBz9wUcw9+8/bFZ1B/4pq29wCMQC0pQWX6zTndljDEL99As1pw
+WntAU9xcq+ffagoH6zDpKUvdxV6Ezj8LcCcPZN6BU=",
  "id": "2fb07c4391d0401696ed345dd1229158",
  "app_id": "db246f3f2ecd45f29ecb0f305e821fdc",
  "create_time": "2019-06-05T04:57:14.470987604Z"
}
```

Status Codes

Table 5-197 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
500	Server Internal Error

5.3.11 Querying AppCode Details

Function

This API is used to query details of a specified AppCode.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-198 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/apps/{app_id}/app-codes/{id}

The following table lists the parameters in the URI.

Table 5-199 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	AppCode ID
app_id	Yes	String	App ID

Request

N/A

Response

Table 5-200 Parameter description

Parameter	Type	Description
id	String	AppCode ID
app_code	String	AppCode value
app_id	String	App ID
create_time	Timestamp	Time when the AppCode is created

Example response:

```
{
  "app_code": "GjOD3g80AABuuFeEJpVQADBlAjBh3UzC7W
+gr4VJBB5BtJ4fdVOQoSvoji3gFxUDb5pWBz9wUcw9+8/bFZ1B/4pq29wCMQC0pQWX6zTndljDEl99As1pw
+WntAU9xcq+ffagoH6zDpKUvdxV6Ezj8LcCcPZN6BU=",
  "id": "2fb07c4391d0401696ed345dd1229158",
  "app_id": "db246f3f2ecd45f29ecb0f305e821fdc",
  "create_time": "2019-06-05T04:57:14.470987604Z"
}
```

Status Codes

Table 5-201 Status codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.3.12 Querying an AppCode List

Function

This API is used to query a list of AppCodes that match specified conditions.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-202 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/apps/{app_id}/app-codes[?page_size, page_no]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **page_size** and **page_no**.

The following table lists the parameters in the URI.

Table 5-203 Parameter description

Parameter	Mandatory	Type	Description
app_id	Yes	String	App ID

Request

N/A

Response

Table 5-204 Parameter description

Parameter	Type	Description
total	Integer	Number of apps that match the query conditions
size	Integer	Length of the returned AppCode list
app_codes	Dictionary	AppCode list

Table 5-205 Parameter description of app_codes

Parameter	Type	Description
id	String	AppCode ID
app_code	String	AppCode value
app_id	String	App ID
create_time	Timestamp	Time when the AppCode is created

Example response:

```
{
  "total": 4,
  "size": 4,
  "app_codes": [
    {
      "app_code": "7049bc6b5b4140b4a93340f2555641bbc4cc7179e7734baeb85a773041cbfb1a",
      "id": "5434c97d872f41a88b039a8a973e0652",
      "app_id": "db246f3f2ecd45f29ecb0f305e821fdc",
      "create_time": "2019-06-05T08:54:25Z"
    },
    {
      "app_code": "asdssdadassssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss",
      "id": "787860297c3d4e51b76fff8abd089a94",
      "app_id": "db246f3f2ecd45f29ecb0f305e821fdc",
      "create_time": "2019-06-05T04:56:51Z"
    },
    {
      "app_code": "MeOAgeemgeatouS7peiwg+ivleaooeW8j+aJp+ihjHNoZWxs6lSa5pyslCAGLS0tLS0tLS3lronoo4XljiXmrovnlZnvvlzkulvkuKrniYjmnKzlop7liqDpg6jnvbLlronoo4XljiXliKDpmaQ2222221234124",
      "id": "c7a87cdfa50b4a4eaa644901c4dddb98",
      "app_id": "db246f3f2ecd45f29ecb0f305e821fdc",
      "create_time": "2019-05-10T03:14:02Z"
    }
  ]
}
```

```
"app_code": "MeOAgeemgeatouS7peiwg+ivleaooeW8j+aJp  
+ihjHNoZWxs6lSa5pyslCAgLS0tLS0tLS3lronoo4XljlXmrovnIznvvlzkulvkuKrniYjmnKzlop7liqDpg6jnvbLlronoo4  
XljlXliKDpmaQ",  
  "id": "7be28fde162b4186a9a07543ca48a28e",  
  "app_id": "db246f3f2ecd45f29ecb0f305e821fdc",  
  "create_time": "2019-05-10T03:13:27Z"  
}  
]  
}
```

Status Codes

Table 5-206 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
500	Server Internal Error

5.3.13 Deleting an AppCode

Function

This API is used to delete a specified AppCode. After the AppCode is deleted, the corresponding API cannot be called through AppCode authentication.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-207 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/apps/{app_id}/app-codes/{id}

The following table lists the parameters in the URI.

Table 5-208 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	AppCode ID
app_id	Yes	String	App ID

Request

N/A

Response

N/A

Status Codes

Table 5-209 Status codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
409	Conflict
500	Server Internal Error

5.4 App Authorization Management

5.4.1 Object Model

This section describes the object model for app authorization.

 NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of C is mandatory.

Table 5-210 Object model for app authorization

Parameter	Type	Description	Operation Type	Mandatory
id	String	Authorization ID	R	-
app_id	String	App ID	CR	Yes
front_api_id	String	API ID	CR	Yes

Parameter	Type	Description	Operation Type	Mandatory
env_id	String	ID of the environment in which the API is published	CR	Yes
create_time	Timestamp	Authorization time	R	-
auth_role	String	Authorizer	R	-

5.4.2 Querying the List of APIs Not Bound to an App

Function

This API is used to query the list of self-developed APIs that have not been bound to an app in a specified environment.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-211 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/app-auths/unbinded-apis[?page_size, page_no, app_id, env_id, api_id, api_name, group_id]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **app_id**, **api_id**, **api_name**, **group_id**, **env_id**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-212 Parameter description

Parameter	Mandatory	Type	Description
app_id	Yes	String	App ID
env_id	Yes	String	Environment ID
group_id	No	String	API group ID

Parameter	Mandatory	Type	Description
api_id	No	String	API ID
api_name	No	String	API name
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .

Request

N/A

Response

Table 5-213 Parameter description

Parameter	Type	Description
total	Integer	Number of APIs that match the query conditions
size	Integer	Length of the returned API list
apis	Dictionary	API list

Table 5-214 Parameter description of apis

Parameter	Type	Description
id	String	API ID
name	String	API name
group_id	String	ID of the API group to which the API belongs
group_name	String	Name of the API group to which the API belongs
remark	String	Description of the API
run_env_name	String	Name of the environment in which the API has been published
run_env_id	String	ID of the environment in which the API has been published
publish_id	String	ID of the publication record

Parameter	Type	Description
auth_type	String	Security authentication mode
req_uri	String	Access address

Example response:

```
{
  "total": 1,
  "size": 1,
  "apis": [{
    "id": "5bbc47e2-95b0-4a56-904e-a3cdc422f8e9",
    "name": "API_group_list_query",
    "remark": "API group list query",
    "group_id": "73c58022-f20d-495a-a188-85d718647f09",
    "group_name": "api_group_001",
    "run_env_name": "RELEASE",
    "run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "publish_id": "65e6fe53-1ac3-4481-ba36-9f0bc6f22057",
    "auth_type": "APP",
    "req_uri": "/test"
  }]
}
```

Status Codes

Table 5-215 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.4.3 Authorizing Apps

Function

An app cannot access any APIs immediately after it is created. To access an API in an environment, first authorize the app to call the API.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-216 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/app-auths

Request

Table 5-217 Parameter description

Parameter	Mandatory	Type	Description
api_ids	Yes	Array of strings	List of API IDs
app_ids	Yes	Array of strings	List of app IDs
env_id	Yes	String	ID of the environment in which the apps will be authorized

Example request:

```
{
  "api_ids": ["5bbc47e2-95b0-4a56-904e-a3cdc422f8e9",
    "6632a062-9dcf-4f18-9646-3cabb925a290"],
  "app_ids": ["14b399ac-967f-4115-bb62-c0346b4537e9"],
  "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID"
}
```

Response

Table 5-218 Parameter description

Parameter	Type	Description
--	Dictionary	Authorization list

Table 5-219 Parameter description of the authorization list

Parameter	Type	Description
id	String	Authorization ID
api_id	String	API ID
app_id	String	App ID
auth_time	Timestamp	Authorization time

Parameter	Type	Description
auth_role	String	Authorizer, which can be: PROVIDER CONSUMER
auth_result	String	Authorization result, which can be: SUCCESS SKIPPED

Example response:

```
[{
  "id": "dffcaff92d144135a9f420fcd485bbf3",
  "api_id": "8aa097b00e9843efabc9c593d11b769d",
  "app_id": "f8c6ea15-0d1b-4c5b-bd4b-911610bd3b3e",
  "auth_time": "2018-03-30T09:37:43.490197204Z",
  "auth_role": "PROVIDER",
  "auth_result": "SUCCESS"
}]
```

Status Codes

Table 5-220 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
409	Conflict
500	Server Internal Error

5.4.4 Querying the List of APIs Bound to an App

Function

This API is used to query the list of APIs that have been bound to a specified app.

 NOTE

Only APIs that an app has been authorized to access in an environment can be queried.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-221 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/app-auths/binded-apis[?page_size, page_no, app_id, api_id, api_name, group_id, group_name, env_id]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **app_id**, **api_id**, **api_name**, **group_id**, **group_name**, **env_id**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-222 Parameter description

Parameter	Mandatory	Type	Description
app_id	Yes	String	App ID
api_id	No	String	API ID
api_name	No	String	API name
group_id	No	String	API group ID
group_name	No	String	API group name
env_id	No	String	ID of the environment in which the app has been authorized
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .

Request

N/A

Response

Table 5-223 Parameter description

Parameter	Type	Description
total	Integer	Number of APIs that match the query conditions
size	Integer	Length of the returned API list
auths	Dictionary	API list

Table 5-224 Parameter description of auths

Parameter	Type	Description
id	String	Authorization ID
api_id	String	API ID
api_name	String	API name
group_name	String	API group to which the API belongs
api_remark	String	Description of the API
api_type	Integer	API type
envname	String	Name of the environment in which the app has been authorized to call the API
env_id	String	ID of the environment
auth_role	String	Authorizer
auth_time	String	Authorization time
appid	String	App ID
app_name	String	App name
app_creator	String	App creator, which can be: ● USER: tenant ● MARKET: API marketplace
app_remark	String	App description
app_type	String	App type
publish_id	String	API publication ID

Example response:

```
{  
  "total": 1,
```

```
"size": 1,
"auths": [{
  "id": "cfa688d8-094b-445a-b270-6aeb0b70a84a",
  "api_id": "6632a062-9dcf-4f18-9646-3cabb925a290",
  "api_name": "API_list_query",
  "group_name": "api_group_001",
  "api_type": 1,
  "api_remark": "API list query",
  "envname": "RELEASE",
  "auth_role": "PROVIDER",
  "auth_time": "2017-12-28T12:46:43Z",
  "appid": "14b399ac-967f-4115-bb62-c0346b4537e9",
  "app_name": "app_001",
  "app_creator": "USER",
  "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "app_remark": "App description",
  "app_type": "apig",
  "publish_id": "f500ba7e369b4b1ebae99aa9d114a17a"
}]
}
```

Status Codes

Table 5-225 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.4.5 Querying the List of Apps Bound to an API

Function

This API is used to query the list of apps that have been bound to a specified API.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-226 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/app-auths/binded-apps[?page_size, page_no, api_id, app_name, app_id, env_id]

 NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **api_id**, **app_name**, **app_id**, **env_id**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-227 Parameter description

Parameter	Mandatory	Type	Description
api_id	No	String	API ID
app_name	No	string	App name
app_id	No	String	App ID
env_id	No	String	Environment ID
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .

Request

N/A

Response

Table 5-228 Parameter description

Parameter	Type	Description
total	Integer	Number of apps that match the query conditions
size	Integer	Length of the returned app list
auths	Dictionary	App list

Table 5-229 Parameter description of auths

Parameter	Type	Description
id	String	Authorization ID
api_id	String	API ID

Parameter	Type	Description
api_name	String	API name
group_name	String	API group to which the API belongs
api_remark	String	Description of the API
api_type	Integer	API type
envname	String	Environment in which access to the API has been authorized to an app
auth_role	String	Authorizer
auth_time	String	Authorization time
appid	String	App ID
app_name	String	App name
app_creator	String	App creator, which can be: ● USER: tenant ● MARKET: API marketplace
publish_id	String	ID of the publication record
env_id	String	Environment ID
app_remark	String	App description
app_type	String	App type

Example response:

```
{
  "total": 1,
  "size": 1,
  "auths": [{
    "id": "cfa688d8-094b-445a-b270-6aeb0b70a84a",
    "api_id": "6632a062-9dcf-4f18-9646-3cabb925a290",
    "api_name": "API_list_query",
    "group_name": "api_group_001",
    "api_type": 1,
    "api_remark": "API list query",
    "envname": "RELEASE",
    "auth_role": "PROVIDER",
    "auth_time": "2017-12-28T12:46:43Z",
    "appid": "14b399ac-967f-4115-bb62-c0346b4537e9",
    "app_name": "app_001",
    "app_creator": "USER",
    "publish_id": "fe9d8ea9f9424594abc3bbe8d861c0f0",
    "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "app_remark": "",
    "app_type": "apig"
  }]
}
```


Status Codes

Table 5-230 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.4.6 Canceling Authorization

Function

This API is used to cancel the authorization of an app for accessing an API. After this operation, the app can no longer call the API.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-231 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/app-auths/{id}

The following table lists the parameter in the URI.

Table 5-232 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Authorization ID

Request

N/A

Response

N/A

Status Codes

Table 5-233 Status codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.5 Environment Management

5.5.1 Object Model

This section describes the object model for environment management.

 NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of C is mandatory.

Table 5-234 Object model for environment management

Parameter	Type	Description	Operation Type	Mandatory
id	String	Environment ID	R	-
name	String	Environment name	CUR	Yes
alias	String	Environment alias	RU	-
project_id	String	ID of the tenant that creates the environment	-	-
create_time	String	Time when the environment is created	R	-
remark	String	Description of the environment	CUR	No

5.5.2 Creating an Environment

Function

API providers can publish an API in different environments, such as the development, test, and production environments. API information, such as the version, request address, and even request message, varies depending on the environment in which an API is published. For example, v1.0 of an API is published in the production environment, v1.1 in the test environment, and v1.2 in the development environment.

APIG provides environment management, enabling you to access APIG in different scenarios at minimal costs.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-235 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/envs

Request

Table 5-236 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	Environment name An environment name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
remark	No	String	Description of the environment The description cannot exceed 255 characters.

Example request:

```
{
  "name": "DEV",
  "remark": "Development environment"
}
```

Response

Table 5-237 Parameter description

Parameter	Type	Description
id	String	Environment ID
name	String	Environment name
create_time	Timestamp	Time when the environment is created
remark	String	Description of the environment

Example response:

```
{
  "id": "0035dd2e76dd4e3fa45fef634318ada4",
  "name": "DEV",
  "remark": "Development environment",
  "create_time": "2017-12-28T12:50:47.0744311Z"
}
```

Status Codes

Table 5-238 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
500	Server Internal Error

5.5.3 Modifying an Environment

Function

This API is used to modify the information about a specified environment. Only the **name** and **remark** attributes of an environment can be modified.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-239 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/envs/{id}

The following table lists the parameter in the URI.

Table 5-240 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Environment ID, which can be obtained by querying the environment information

Request

Table 5-241 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	Environment name An environment name consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
remark	No	String	Description of the environment The description cannot exceed 255 characters.

Example request:

```
{
  "name": "DEVELOP",
  "remark": "Development environment"
}
```

Response

Table 5-242 Parameter description

Parameter	Type	Description
id	String	Environment ID

Parameter	Type	Description
name	String	Environment name
create_time	Timestamp	Time when the environment is created
remark	String	Description of the environment

Example response:

```
{
  "id": "0035dd2e76dd4e3fa45fef634318ada4",
  "name": "DEVELOP",
  "remark": "Development environment",
  "create_time": "2017-12-28T12:50:47Z"
}
```

Status Codes

Table 5-243 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.5.4 Deleting an Environment

Function

This API is used to delete a specified environment.

This operation will cause the APIs published in the environment to become inaccessible to relevant apps and users. Ensure that you have notified users of the deletion or confirm that you insist on removing APIs from the deleted environment.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-244 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/envs/{id}

The following table lists the parameter in the URI.

Table 5-245 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Environment ID

Request

N/A

Response

N/A

Status Codes

Table 5-246 Status codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.5.5 Querying an Environment List

Function

This API is used to query an environment list that matches specified conditions.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-247 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/envs[?page_no, page_size,name]

 NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **name**, **page_size**, and **page_no**.

Table 5-248 Parameter description

Parameter	Mandatory	Type	Description
name	No	String	Environment name.
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .
precise_search	No	String	Parameter name (name supported only) for exact match.

Request

N/A

Response**Table 5-249** Parameter description

Parameter	Type	Description
total	Integer	Number of environments that match the query conditions
size	Integer	Length of the returned environment list
envs	Dictionary	Environment list

Table 5-250 Parameter description of envs

Parameter	Type	Description
id	String	Environment ID
name	String	Environment name
create_time	Timestamp	Time when the environment is created
remark	String	Description of the environment

Example response:

```
{
  "total": 2,
  "size": 2,
  "envs": [{
    "id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "name": "RELEASE",
    "remark": "Production environment",
    "create_time": "2017-12-29T03:39:03.165657Z"
  },
  {
    "id": "0035dd2e76dd4e3fa45fef634318ada4",
    "name": "DEVELOP",
    "remark": "Development environment",
    "create_time": "2017-12-28T12:50:47Z"
  }
]}
```

Status Codes

Table 5-251 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
500	Server Internal Error

5.6 Environment Variable Management

5.6.1 Object Model

This section describes the environment variable object model.

 NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of C is mandatory.

Table 5-252 Environment variable object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Environment variable ID	R	-
env_id	String	Environment ID	CR	Yes
group_id	String	API group ID	CR	Yes
variable_name	String	Variable name	CR	Yes
variable_value	String	Variable value	CR	Yes

5.6.2 Creating an Environment Variable

Function

Publishing an API in different environments may involve various environment variables, such as API service deployment address and request version.

Define environment variables when creating an API. When the API is called, the environment variables will be replaced with the variable values to distinguish environments.

Environment variables are defined for an API group and apply to all APIs in the group.

 NOTE

1. Environment variable names must be unique for an API group in the same environment.
2. Environment variable names are case-sensitive. For example, **ABC** and **abc** are two different variables.
3. APIs that use environment variables cannot be debugged.
4. You must enclose an environment variable in number signs (#) so that it can be replaced with the actual value of the environment in which the API is published. For example, if the URL of an API is <https://#address#:8080> and the value of variable **address** is **192.168.1.5** in the RELEASE environment, the real URL of the API is **https://192.168.1.5:8080** after publishing.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-253 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/env-variables

Request

Table 5-254 Parameter description

Parameter	Mandatory	Type	Description
env_id	Yes	String	Environment ID
group_id	Yes	String	API group ID
variable_name	Yes	String	Variable name A variable name consists of 3–32 characters, starting with a letter. Only letters, digits, hyphens (-), and underscores (_) are allowed. The variable name is equivalent to #Name# in an API definition. Characters between the number signs are case-sensitive. The variable name will be replaced with the variable value after API publishing.
variable_value	Yes	String	Variable value A variable value consists of 1–255 characters. Only letters, digits, and special characters (_-/:.) are allowed.

Example request:

```
{
  "env_id": "cca3616af3684b329064b2a631cb3eeb",
  "group_id": "73c58022f20d495aa18885d718647f09",
  "variable_name": "address",
  "variable_value": "192.168.1.5"
}
```

Response

Table 5-255 Parameter description

Parameter	Type	Description
id	String	Environment variable ID
env_id	String	Environment ID

Parameter	Type	Description
group_id	String	API group ID
variable_name	String	Variable name
variable_value	String	Variable value

Example response:

```
{
  "id": "104185e53e8f4c63a7e5ef4117bf870c",
  "env_id": "cca3616af3684b329064b2a631cb3eeb",
  "group_id": "73c58022f20d495aa18885d718647f09",
  "variable_name": "address",
  "variable_value": "192.168.1.5"
}
```

Status Codes

Table 5-256 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.6.3 Deleting an Environment Variable

Function

This API is used to delete a specified environment variable.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-257 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/env-variables/{id}

The following table lists the parameter in the URI.

Table 5-258 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Environment variable ID

Request

N/A

Response

N/A

Status Codes

Table 5-259 Status codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.6.4 Querying Environment Variable Details

Function

This API is used to query the details of an environment variable.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-260 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/env-variables/{id}

The following table lists the parameter in the URI.

Table 5-261 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Environment variable ID

Request

N/A

Response

Table 5-262 Parameter description

Parameter	Type	Description
id	String	Environment variable ID
env_id	String	Environment ID
group_id	String	API group ID
variable_name	String	Variable name
variable_value	String	Variable value

Example response:

```
{
  "id": "104185e53e8f4c63a7e5ef4117bf870c",
  "env_id": "cca3616af3684b329064b2a631cb3eeb",
  "group_id": "73c58022f20d495aa18885d718647f09",
  "variable_name": "address",
  "variable_value": "192.168.1.5"
}
```

Status Codes

Table 5-263 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.6.5 Querying an Environment Variable List

Function

This API is used to query the list of all environment variables under an API group.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-264 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/env-variables[?page_size, page_no, env_id, group_id, variable_name]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **env_id**, **group_id**, **variable_name**, **page_size**, and **page_no**.

Table 5-265 Parameter description

Parameter	Mandatory	Type	Description
env_id	No	String	Environment ID
group_id	Yes	String	API group ID
variable_name	No	String	Variable name

Parameter	Mandatory	Type	Description
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .
precise_search	No	String	Parameter name (variable_name) for exact matching

Request

N/A

Response

Table 5-266 Parameter description

Parameter	Type	Description
variables	Dictionary	Environment variable list
total	Integer	Number of environment variables that match the query conditions
size	Integer	Length of the returned environment variable list

Table 5-267 Parameter description of variables

Parameter	Type	Description
id	String	Environment variable ID
env_id	String	Environment ID
group_id	String	API group ID
variable_name	String	Variable name
variable_value	String	Variable value

Example response:


```
{
  "total": 2,
  "size": 2,
  "variables": [{
    "id": "09ab8135722440b9bf5d107f2a09d409",
    "env_id": "cca3616af3684b329064b2a631cb3eeb",
    "group_id": "73c58022f20d495aa18885d718647f09",
    "variable_name": "port",
    "variable_value": "8080"
  },
  {
    "id": "104185e53e8f4c63a7e5ef4117bf870c",
    "env_id": "cca3616af3684b329064b2a631cb3eeb",
    "group_id": "73c58022f20d495aa18885d718647f09",
    "variable_name": "address",
    "variable_value": "192.168.1.5"
  }
  ]
}
```

Status Codes

Table 5-268 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.7 Request Throttling Policy Management

5.7.1 Object Model

This section describes the request throttling policy object model.

 NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of C is mandatory.

Table 5-269 Request throttling policy object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	ID of a request throttling policy	R	-
name	String	Name of a request throttling policy	CRU	Yes
project_id	String	ID of the tenant that creates the request throttling policy	-	-
api_call_limits	Integer	Maximum number of times an API can be accessed within a specified period	CRU	Yes
user_call_limits	Integer	Maximum number of times the API can be accessed by a user within the same period. The value of this parameter must be less than or equal to that of api_call_limits .	CRU	No
app_call_limits	Integer	Maximum number of times the API can be accessed by an app within the same period. The value of this parameter must be less than or equal to that of user_call_limits .	CRU	No
ip_call_limits	Integer	Maximum number of times the API can be accessed by an IP address within the same period. The value of this parameter must be less than or equal to that of api_call_limits .	CRU	No
time_interval	Integer	Period of time for limiting the number of API calls	CRU	Yes

Parameter	Type	Description	Operation Type	Mandatory
time_unit	String	Time unit, which can be: • SECOND • MINUTE • HOUR • DAY	CRU	Yes
create_time	Timestamp	Time when the request throttling policy is created	R	-
remark	String	Description of the request throttling policy	CRU	No
type	Integer	Type of the request throttling policy, which can be: • 1: exclusive • 2: shared	CRU	No

5.7.2 Creating a Request Throttling Policy

Function

After an API goes online, the system attaches a request throttling policy to it by default. The API provider can change the request throttling policy based on the service capabilities and load of the API.

A request throttling policy restricts the maximum number of times an API can be called within a specified period.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-270 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/throttles

Request

Table 5-271 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	Name of the request throttling policy The name of a request throttling policy consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
api_call_limits	Yes	Integer	Maximum number of times an API can be accessed within a specified period. The value of this parameter cannot exceed the default limit 200 TPS. You can change the default limit to meet service requirements. The maximum value is 2,147,483,647. Enter a positive integer.
user_call_limits	No	Integer	Maximum number of times the API can be accessed by a user within the same period. The value of this parameter must be less than or equal to that of api_call_limits . The maximum value is 2,147,483,647. Enter a positive integer.
app_call_limits	No	Integer	Maximum number of times the API can be accessed by an app within the same period. The value of this parameter must be less than or equal to that of user_call_limits . The maximum value is 2,147,483,647. Enter a positive integer.
ip_call_limits	No	Integer	Maximum number of times the API can be accessed by an IP address within the same period. The value of this parameter must be less than or equal to that of api_call_limits . The maximum value is 2,147,483,647. Enter a positive integer.
time_interval	Yes	Integer	Period of time for limiting the number of API calls. This parameter applies with each of the preceding three API call limits. The maximum value is 2,147,483,647. Enter a positive integer.
time_unit	Yes	String	Time unit, which can be: • SECOND • MINUTE • HOUR • DAY

Parameter	Mandatory	Type	Description
remark	No	String	Description of the request throttling policy The description cannot exceed 255 characters.
type	No	Integer	Type of the request throttling policy, which can be: • 1: exclusive, limiting the maximum number of times a single API can be called within the specified period. • 2: shared, limiting the maximum number of times all APIs can be called within the specified period.
enable_adaptive_control	No	String	Enabling status of dynamic request throttling • TRUE • FALSE This function is currently not available.

Example request:

```
{
  "api_call_limits": 800,
  "user_call_limits": 500,
  "app_call_limits": 300,
  "ip_call_limits": 600,
  "name": "800_calls_per_second",
  "remark": "Total: 800 calls/second; user: 500 calls/second; app: 300 calls/second; IP address: 600 calls/second",
  "time_interval": 1,
  "time_unit": "SECOND"
}
```

Response

Table 5-272 Parameter description

Parameter	Type	Description
id	String	ID of the request throttling policy
name	String	Name of the request throttling policy
api_call_limits	Integer	Maximum number of times an API can be accessed within a specified period
user_call_limits	Integer	Maximum number of times the API can be accessed by a user within the same period
app_call_limits	Integer	Maximum number of times the API can be accessed by an app within the same period

Parameter	Type	Description
ip_call_limits	Integer	Maximum number of times the API can be accessed by an IP address within the same period
time_interval	Integer	Period of time for limiting the number of API calls
time_unit	String	Time unit for limiting the number of API calls
remark	String	Description of the request throttling policy
create_time	Timestamp	Time when the request throttling policy is created
is_include_special_throttle	Integer	Indicates whether an excluded request throttling configuration has been created. The value can be: • 1: yes • 2: no
type	Integer	Type of the request throttling policy, which can be: • 1: exclusive • 2: shared
bind_num	Integer	Number of APIs to which the request throttling policy has been bound
enable_adaptive_control	String	Enabling status of dynamic request throttling • TRUE • FALSE This function is currently not available.

Example response:

```
{
  "id": "0325b671-2d50-4614-9868-22102262695d",
  "name": "800_calls_per_second",
  "api_call_limits": 800,
  "user_call_limits": 500,
  "app_call_limits": 300,
  "ip_call_limits": 600,
  "time_interval": 1,
  "time_unit": "SECOND",
  "create_time": "2017-12-29T01:55:59.9904225Z",
  "remark": "Total: 800 calls/second; user: 500 calls/second; app: 300 calls/second; IP address: 600 calls/second",
  "is_inclu_special_throttle": 2,
  "type": 1,
  "bind_num": 0,
  "enable_adaptive_control": "FALSE"
}
```

Status Codes

Table 5-273 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
500	Server Internal Error

5.7.3 Modifying a Request Throttling Policy

Function

This API is used to modify the detailed information of a request throttling policy.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-274 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/throttles/{id}

The following table lists the parameter in the URI.

Table 5-275 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the request throttling policy that you want to modify

Request

Table 5-276 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	Name of the request throttling policy that you want to modify The name of a request throttling policy consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
api_call_limits	Yes	Integer	Maximum number of times an API can be accessed within a specified period. The value of this parameter cannot exceed the default limit 200 TPS. You can change the default limit to meet service requirements. The maximum value is 2,147,483,647. Enter a positive integer.
user_call_limits	No	Integer	Maximum number of times the API can be accessed by a user within the same period. The value of this parameter must be less than or equal to that of api_call_limits . The maximum value is 2,147,483,647. Enter a positive integer.
app_call_limits	No	Integer	Maximum number of times the API can be accessed by an app within the same period. The value of this parameter must be less than or equal to that of user_call_limits . The maximum value is 2,147,483,647. Enter a positive integer.
ip_call_limits	No	Integer	Maximum number of times the API can be accessed by an IP address within the same period. The value of this parameter must be less than or equal to that of api_call_limits . The maximum value is 2,147,483,647. Enter a positive integer.
time_interval	Yes	Integer	Period of time for limiting the number of API calls. This parameter applies with each of the preceding three API call limits. The maximum value is 2,147,483,647. Enter a positive integer.

Parameter	Mandatory	Type	Description
time_unit	Yes	String	Time unit, which can be: • SECOND • MINUTE • HOUR • DAY
remark	No	String	Description of the request throttling policy The description cannot exceed 255 characters.
type	No	Integer	Type of the request throttling policy, which can be: • 1: exclusive, limiting the maximum number of times a single API can be called within the specified period. • 2: shared, limiting the maximum number of times all APIs can be called within the specified period.
enable_adaptive_control	No	String	Enabling status of dynamic request throttling • TRUE • FALSE This function is currently not available.

Example request:

```
{
  "api_call_limits": 1000,
  "user_call_limits": 500,
  "app_call_limits": 300,
  "ip_call_limits": 600,
  "name": "1000_calls_per_second",
  "remark": "Total: 1000 calls/second; user: 500 calls/second; app: 300 calls/second; IP address: 600 calls/second",
  "time_interval": 1,
  "time_unit": "SECOND"
}
```

Response

Table 5-277 Parameter description

Parameter	Type	Description
id	String	ID of the request throttling policy
name	String	Name of the request throttling policy

Parameter	Type	Description
api_call_limits	Integer	Maximum number of times an API can be accessed within a specified period
user_call_limits	Integer	Maximum number of times the API can be accessed by a user within the same period
app_call_limits	Integer	Maximum number of times the API can be accessed by an app within the same period
ip_call_limits	Integer	Maximum number of times the API can be accessed by an IP address within the same period
time_interval	Integer	Period of time for limiting the number of API calls
time_unit	String	Time unit for limiting the number of API calls
remark	String	Description of the request throttling policy
create_time	Timestamp	Time when the request throttling policy is created
is_include_special_throttle	Integer	Indicates whether an excluded request throttling configuration has been created. The value can be: • 1: yes • 2: no
type	Integer	Type of the request throttling policy, which can be: • 1: exclusive • 2: shared
bind_num	Integer	Number of APIs to which the request throttling policy has been bound
enable_adaptive_control	String	Enabling status of dynamic request throttling • TRUE • FALSE This function is currently not available.

Example response:

```
{
  "id": "0325b671-2d50-4614-9868-22102262695d",
  "name": "1000_calls_per_second",
  "api_call_limits": 1000,
  "user_call_limits": 500,
  "app_call_limits": 300,
  "ip_call_limits": 600,
  "time_interval": 1,
  "time_unit": "SECOND",
```

```
"create_time": "2017-12-29T01:55:59Z",
"remark": "Total: 1000 calls/second; user: 500 calls/second; app: 300 calls/second; IP address: 600 calls/second",
"is_inclu_special_throttle": 2,
"type": 1,
"bind_num": 0,
"enable_adaptive_control": "FALSE"
}
```

Status Codes

Table 5-278 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.7.4 Deleting a Request Throttling Policy

Function

This API is used to delete a request throttling policy and all binding relationships between the policy and APIs.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-279 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/throttles/{id}

The following table lists the parameter in the URI.

Table 5-280 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	ID of a request throttling policy

Request

N/A

Response

N/A

Status Codes

Table 5-281 Status codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.7.5 Querying Details of a Request Throttling Policy

Function

This API is used to query the details of a request throttling policy.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-282 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/throttles/{id}

The following table lists the parameter in the URI.

Table 5-283 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	ID of a request throttling policy

Request

N/A

Response

Table 5-284 Parameter description

Parameter	Type	Description
id	String	ID of the request throttling policy
name	String	Name of the request throttling policy
api_call_limits	Integer	Maximum number of times an API can be accessed within a specified period
user_call_limits	Integer	Maximum number of times the API can be accessed by a user within the same period
app_call_limits	Integer	Maximum number of times the API can be accessed by an app within the same period
ip_call_limits	Integer	Maximum number of times the API can be accessed by an IP address within the same period
time_interval	Integer	Period of time for limiting the number of API calls
time_unit	String	Time unit for limiting the number of API calls
remark	String	Description of the request throttling policy
create_time	Timestamp	Time when the request throttling policy is created
is_include_special_throttle	Integer	Indicates whether an excluded request throttling configuration has been created. The value can be: 1: yes 2: no

Parameter	Type	Description
type	Integer	Type of the request throttling policy, which can be: • 1: exclusive • 2: shared
bind_num	Integer	Number of APIs to which the request throttling policy has been bound
enable_adaptive_control	String	Enabling status of dynamic request throttling • TRUE • FALSE This function is currently not available.

Example response:

```
{
  "id": "0325b671-2d50-4614-9868-22102262695d",
  "name": "1000_calls_per_second",
  "api_call_limits": 1000,
  "user_call_limits": 500,
  "app_call_limits": 300,
  "ip_call_limits": 600,
  "time_interval": 1,
  "time_unit": "SECOND",
  "create_time": "2017-12-29T01:55:59Z",
  "remark": "Total: 1000 calls/second; user: 500 calls/second; app: 300 calls/second; IP address: 600 calls/second",
  "is_inclu_special_throttle": 2,
  "type": 1,
  "bind_num": 0,
  "enable_adaptive_control": "FALSE"
}
```

Status Codes

Table 5-285 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.7.6 Querying the Request Throttling Policy List

Function

This API is used to query all request throttling policies.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-286 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/throttles[?page_size, page_no, id, name]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **id**, **name**, **page_size**, and **page_no**.

Request

Table 5-287 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	ID of a request throttling policy
name	No	String	Name of the request throttling policy
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .
precise_search	No	String	Parameter name (name) for exact matching

Response

Table 5-288 Parameter description

Parameter	Type	Description
total	Integer	Number of request throttling policies that match the query conditions
size	Integer	Length of the returned request throttling policy list
throttles	Dictionary	Request throttling policy list

Table 5-289 Parameter description of throttles

Parameter	Type	Description
id	String	ID of a request throttling policy
name	String	Name of the request throttling policy
api_call_limits	Integer	Maximum number of times an API can be accessed within a specified period
user_call_limits	Integer	Maximum number of times the API can be accessed by a user within the same period
app_call_limits	Integer	Maximum number of times the API can be accessed by an app within the same period
ip_call_limits	Integer	Maximum number of times the API can be accessed by an IP address within the same period
time_interval	Integer	Period of time for limiting the number of API calls
time_unit	String	Time unit for limiting the number of API calls
remark	String	Description of the request throttling policy
create_time	Timestamp	Time when the request throttling policy is created
is_include_special_throttle	Integer	Indicates whether an excluded request throttling configuration has been created. The value can be: 1: yes 2: no

Parameter	Type	Description
type	Integer	Type of the request throttling policy, which can be: • 1: exclusive • 2: shared
bind_num	Integer	Number of APIs to which the request throttling policy has been bound
enable_adaptive_control	String	Enabling status of dynamic request throttling • TRUE • FALSE This function is currently not available.

Example response:

```
{
  "total": 2,
  "size": 2,
  "throttles": [{
    "id": "a3106cfe-801f-4919-b0d7-d785dc5b47f9",
    "name": "500_calls_per_second",
    "api_call_limits": 500,
    "user_call_limits": 200,
    "app_call_limits": 100,
    "ip_call_limits": 100,
    "time_interval": 1,
    "time_unit": "SECOND",
    "create_time": "2017-12-29T02:04:08Z",
    "remark": "Total: 500 calls/second; user: 200 calls/second; app: 100 calls/second; IP address: 100 calls/second",
    "is_inclu_special_throttle": 2,
    "type": 1,
    "bind_num": 1,
    "enable_adaptive_control": "FALSE"
  },
  {
    "id": "0325b671-2d50-4614-9868-22102262695d",
    "name": "1000_calls_per_second",
    "api_call_limits": 1000,
    "user_call_limits": 500,
    "app_call_limits": 300,
    "ip_call_limits": 600,
    "time_interval": 1,
    "time_unit": "SECOND",
    "create_time": "2017-12-29T01:55:59Z",
    "remark": "Total: 1000 calls/second; user: 500 calls/second; app: 300 calls/second; IP address: 600 calls/second",
    "is_inclu_special_throttle": 2,
    "type": 1,
    "bind_num": 1,
    "enable_adaptive_control": "FALSE"
  }
]}
```

Status Codes

Table 5-290 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
500	Server Internal Error

5.8 Binding Request Throttling Policies

5.8.1 Object Model

This section describes the object model for binding a request throttling policy to an API.

 NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of **C** is mandatory.

Table 5-291 Object model for binding a request throttling policy

Parameter	Type	Description	Operation Type	Mandatory
id	String	Binding ID	R	-
throttle_id	String	Request throttling policy ID	CR	Yes
front_api_id	String	API ID	CR	Yes
env_id	String	Environment ID	CR	Yes
create_time	Timestamp	Time when the request throttling policy is bound to the API	R	-

5.8.2 Querying the List of APIs Not Bound to a Request Throttling Policy

Function

This API is used to query the list of self-developed APIs that are not bound to a request throttling policy. Only published APIs will be displayed.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-292 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/throttle-bindings/unbinded-apis[?page_size, page_no, throttle_id, group_id, env_id, api_id, api_name]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **group_id**, **env_id**, **throttle_id**, **api_id**, **api_name**, **page_size**, and **page_no**.

Request

Table 5-293 Parameter description

Parameter	Mandatory	Type	Description
throttle_id	Yes	String	ID of a request throttling policy
env_id	No	String	Environment ID
group_id	No	String	API group ID
api_id	No	String	API ID
api_name	No	String	API name
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .

Parameter	Mandatory	Type	Description
page_no	No	Integer	Page number. The default value is 1.

Response

Table 5-294 Parameter description

Parameter	Type	Description
total	Integer	Number of APIs that match the query conditions
size	Integer	Length of the returned API list
apis	Dictionary	API list

Table 5-295 Parameter description of apis

Parameter	Type	Description
id	String	API ID
name	String	API name
group_id	String	ID of the API group to which the API belongs
group_name	String	Name of the API group to which the API belongs
type	Integer	API type
remark	String	Description of the API
run_env_name	String	Name of the environment in which the API has been published
run_env_id	String	ID of the environment in which the API has been published
publish_id	String	ID of the publication record
throttle_apply_id	String	Binding ID
throttle_name	String	Name of the request throttling policy bound to the API
apply_time	Timestamp	Time when the request throttling policy is bound to the API
auth_type	String	Security authentication mode

Parameter	Type	Description
req_uri	String	Access address

Example response:

```
{
  "total": 2,
  "size": 2,
  "apis": [{
    "id": "5bbc47e2-95b0-4a56-904e-a3cdc422f8e9",
    "name": "API_group_list_query",
    "type": 1,
    "remark": "API group list query",
    "group_id": "73c58022-f20d-495a-a188-85d718647f09",
    "group_name": "api_group_001",
    "run_env_name": "RELEASE",
    "run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "publish_id": "65e6fe53-1ac3-4481-ba36-9f0bc6f22057",
    "auth_type": "APP",
    "req_uri": "/test"
  },
  {
    "id": "6632a062-9dcf-4f18-9646-3cabb925a290",
    "name": "API_list_query",
    "type": 1,
    "remark": "API list query",
    "group_id": "73c58022-f20d-495a-a188-85d718647f09",
    "group_name": "api_group_001",
    "run_env_name": "RELEASE",
    "run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "publish_id": "374a6d5a-20c7-4ea1-82e1-19fce4556956",
    "auth_type": "APP",
    "req_uri": "/test"
  }
]}
```

Status Codes

Table 5-296 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.8.3 Binding a Request Throttling Policy

Function

The request throttling policy bound to an API will control all access to the API. If the number of API calls within a specified period reaches the limit, subsequent access will be rejected, protecting the backend API from abnormal traffic and ensuring stable service running.

This API is used to bind a request throttling policy to an API that has been published in an environment.

You can bind different request throttling policies to an API in different environments, but can bind only one request throttling policy to the API in each environment.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-297 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/throttle-bindings

Request

Table 5-298 Parameter description

Parameter	Mandatory	Type	Description
publish_ids	Yes	Array of strings	API publication record ID
strategy_id	Yes	String	ID of a request throttling policy

Example request:

```
{
  "publish_ids": [
    "374a6d5a-20c7-4ea1-82e1-19fce4556956",
    "65e6fe53-1ac3-4481-ba36-9f0bc6f22057"
  ],
  "strategy_id": "0325b671-2d50-4614-9868-22102262695d"
}
```

Response

Table 5-299 Parameter description

Parameter	Type	Description
throttle_appl s	Dictionary	Binding list

Table 5-300 Parameter description of throttle_applys

Parameter	Type	Description
id	String	Binding ID
strategy_id	String	ID of a request throttling policy
publish_id	String	API publication record ID
scope	Integer	Scope of the request throttling policy, which can be: • 1: access from users and apps • 2: access from a user • 3: access from an app Currently, only 1 is supported.
apply_time	Timestamp	Time when the request throttling policy is bound to the API

Example response:

```
{
  "throttle_applys": [{
    "id": "507c6a9f-8322-4dc2-8ba5-b4d74e3690d3",
    "strategy_id": "0325b671-2d50-4614-9868-22102262695d",
    "publish_id": "374a6d5a-20c7-4ea1-82e1-19fce4556956",
    "scope": 1,
    "apply_time": "2017-12-29T03:01:11.138456Z"
  },
  {
    "id": "90f05978-06a3-4096-8bea-b5e2fa12b843",
    "strategy_id": "0325b671-2d50-4614-9868-22102262695d",
    "publish_id": "65e6fe53-1ac3-4481-ba36-9f0bc6f22057",
    "scope": 1,
    "apply_time": "2017-12-29T03:01:11.138456Z"
  }
]
```

Status Codes

Table 5-301 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.8.4 Querying the List of APIs Bound to a Request Throttling Policy

Function

This API is used to query the list of APIs to which a specified request throttling policy has been bound.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-302 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/throttle-bindings/binded-apis[?page_size, page_no, throttle_id, env_id, group_id, api_id, api_name]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **group_id**, **env_id**, **throttle_id**, **api_id**, **api_name**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-303 Parameter description

Parameter	Mandatory	Type	Description
throttle_id	Yes	String	ID of a request throttling policy
env_id	No	String	Environment ID
group_id	No	String	API group ID
api_id	No	String	API ID
api_name	No	String	API name
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .

Request

N/A

Response

Table 5-304 Parameter description

Parameter	Type	Description
total	Integer	Number of APIs that match the query conditions
size	Integer	Length of the returned API list
apis	Dictionary	API list

Table 5-305 Parameter description of apis

Parameter	Type	Description
id	String	API ID
name	String	API name
group_id	String	ID of the API group to which the API belongs
group_name	String	Name of the API group to which the API belongs
type	Integer	API type

Parameter	Type	Description
remark	String	Description of the API
run_env_name	String	Name of the environment in which the API has been published
run_env_id	String	ID of the environment in which the API has been published
publish_id	String	ID of the publication record
throttle_apply_id	String	Binding ID
throttle_name	String	Name of the request throttling policy bound to the API
apply_time	Timestamp	Time when the request throttling policy is bound to the API
auth_type	String	Security authentication mode
req_uri	String	Access address

Example response:

```
{
  "total": 2,
  "size": 2,
  "apis": [
    {
      "id": "5bbc47e2-95b0-4a56-904e-a3cdc422f8e9",
      "name": "API_group_list_query",
      "type": 1,
      "remark": "API group list query",
      "group_id": "73c58022-f20d-495a-a188-85d718647f09",
      "group_name": "api_group_001",
      "run_env_name": "RELEASE",
      "run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
      "publish_id": "65e6fe53-1ac3-4481-ba36-9f0bc6f22057",
      "throttle_apply_id": "90f05978-06a3-4096-8bea-b5e2fa12b843",
      "throttle_name": "throttle1",
      "apply_time": "2017-12-29T03:01:11.138456Z",
      "auth_type": "APP",
      "req_uri": "/test"
    },
    {
      "id": "6632a062-9dcf-4f18-9646-3cabb925a290",
      "name": "API_list_query",
      "type": 1,
      "remark": "API list query",
      "group_id": "73c58022-f20d-495a-a188-85d718647f09",
      "group_name": "api_group_001",
      "run_env_name": "RELEASE",
      "run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
      "publish_id": "374a6d5a-20c7-4ea1-82e1-19fce4556956",
      "throttle_apply_id": "507c6a9f-8322-4dc2-8ba5-b4d74e3690d3",
      "throttle_name": "throttle1",
      "apply_time": "2017-12-29T03:01:11.138456Z",
      "auth_type": "APP",
      "req_uri": "/test"
    }
  ]
}
```

Status Codes

Table 5-306 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.8.5 Querying the List of Request Throttling Policies Bound to an API

Function

This API is used to query the list of request throttling policies that have been bound to an API. Only one request throttling policy can be bound to an API in an environment.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-307 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/throttle-bindings/binded-throttles[?page_no, page_size, api_id, throttle_id, throttle_name, env_id]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **api_id**, **throttle_id**, **throttle_name**, **env_id**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-308 Parameter description

Parameter	Mandatory	Type	Description
api_id	Yes	String	API ID
throttle_id	No	String	Request throttling policy ID
throttle_name	No	String	Request throttling policy name
env_id	No	String	Environment ID
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .

Request

N/A

Response

Table 5-309 Parameter description

Parameter	Type	Description
total	Integer	Number of request throttling policies that match the query conditions
size	Integer	Length of the returned request throttling policy list
throttles	Dictionary	Request throttling policy list

Table 5-310 Parameter description of throttles

Parameter	Type	Description
id	String	Request throttling policy ID
name	String	Request throttling policy name
api_call_limits	Integer	Maximum number of times an API can be accessed within a specified period

Parameter	Type	Description
user_call_limits	Integer	Maximum number of times the API can be accessed by a user within the same period
app_call_limits	Integer	Maximum number of times the API can be accessed by an app within the same period
ip_call_limits	Integer	Maximum number of times the API can be accessed by an IP address within the same period
time_interval	Integer	Period of time for limiting the number of API calls
time_unit	String	Time unit for limiting the number of API calls
remark	String	Description of the request throttling policy
create_time	Timestamp	Time when the request throttling policy is created
is_include_special_throttle	Integer	Indicates whether an excluded request throttling configuration has been created. The value can be: 1 : yes 2 : no
env_name	String	Environment in which the request throttling policy takes effect
type	Integer	Type of the request throttling policy
bind_id	String	Binding ID
bind_time	Timestamp	Time when the request throttling policy is bound to the API
bind_num	Integer	Number of APIs to which the request throttling policy has been bound
enable_adaptive_control	String	Enabling status of dynamic request throttling. This function is currently not available.

Example response:

```
{
  "total": 1,
  "size": 1,
  "throttles": [{
    "id": "0325b671-2d50-4614-9868-22102262695d",
    "name": "1000_calls_per_second",
    "api_call_limits": 1000,
    "user_call_limits": 500,
    "app_call_limits": 300,
    "ip_call_limits": 100,
    "time_interval": 1,
    "time_unit": "SECOND",
    "create_time": "2017-12-29T01:55:59Z",
```

```
"remark": "Total: 1000 calls/second; user: 500 calls/second; app: 300 calls/second",
"is_inclu_special_throttle": 2,
"env_name": "RELEASE",
  "type": 1,
  "bind_id": "359f5c1868f647b6ad0f0d285154a791",
  "bind_time": "2019-07-08T01:27:38Z",
  "bind_num": 1,
  "enable_adaptive_control": "FALSE"
}]
}
```

Status Codes

Table 5-311 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.8.6 Unbinding a Request Throttling Policy

Function

This API is used to unbind a request throttling policy from an API.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-312 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/throttle-bindings/{id}

The following table lists the parameters in the URI.

Table 5-313 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Binding ID

Request

N/A

Response

N/A

Status Codes

Table 5-314 Status codes

Status Code	Description
204	No Content
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.9 Excluded Request Throttling Configuration

5.9.1 Object Model

This section describes the object model for excluded request throttling configurations.

NOTE

- Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- Mandatory** indicates whether a field with the **Operation Type** of C is mandatory.

Table 5-315 Object model for excluded request throttling configurations

Parameter	Type	Description	Operation Type	Mandatory
id	String	Excluded request throttling configuration ID	R	-
strategy_id	String	Request throttling policy ID	CR	Yes

Parameter	Type	Description	Operation Type	Mandatory
instance_id	String	ID of the object to which the excluded request throttling configuration applies	CR	Yes
instance_type	String	Object type, which can be APP or USER .	CR	Yes
call_limits	Integer	Maximum number of times the excluded object can access an API within the throttling period	CRU	Yes
apply_time	Timestamp	Time when the excluded request throttling configuration is created	R	-

5.9.2 Creating an Excluded Request Throttling Configuration

Function

A request throttling policy controls the maximum number of times an API can be accessed within a specified period and the maximum numbers of times the API can be accessed by a tenant or an app within the same period.

When necessary, you can create an excluded request throttling configuration to specify the threshold of API calls for a specific app. For example, after you set the API call threshold for all apps to 500 calls/minute, you can specify the API call threshold of app 1 as 800 calls/minute.

You can add excluded apps or tenants to a request throttling policy.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-316 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/throttle-specials

Request

Table 5-317 Parameter description

Parameter	Mandatory	Type	Description
call_limits	Yes	Integer	Maximum number of times the excluded object can access an API within the throttling period
instance_id	Yes	String	Excluded app ID or excluded account ID
instance_type	Yes	String	Object type, which can be APP or USER
strategy_id	Yes	String	Request throttling policy ID

Example request:

```
{
  "call_limits": 150,
  "instance_id": "98efd77d-10b5-4eca-8170-ed30a4a286a4",
  "instance_type": "APP",
  "strategy_id": "a3106cfe-801f-4919-b0d7-d785dc5b47f9"
}
```

Response

Table 5-318 Parameter description

Parameter	Type	Description
id	String	Excluded request throttling configuration ID
strategy_id	String	Request throttling policy ID
instance_id	Integer	Excluded object ID
instance_name	String	Name of an app or a tenant to which the excluded request throttling configuration applies
instance_type	Integer	Type of the excluded object
call_limits	Integer	Maximum number of times the excluded object can access an API within the throttling period
apply_time	Timestamp	Time when the excluded request throttling configuration is created
app_id	String	ID of the app to which the excluded request throttling configuration applies

Parameter	Type	Description
app_name	String	Name of the app to which the excluded request throttling configuration applies

Example response:

```
{
  "id": "778879b8-df10-495b-a087-874859fdea6d",
  "strategy_id": "a3106cfe-801f-4919-b0d7-d785dc5b47f9",
  "instance_id": "98efd77d-10b5-4eca-8170-ed30a4a286a4",
  "instance_name": "app_002",
  "instance_type": "APP",
  "call_limits": 150,
  "apply_time": "2017-12-29T03: 11: 18.2698381Z",
  "app_id": "98efd77d-10b5-4eca-8170-ed30a4a286a4",
  "app_name": "app_002"
}
```

Status Codes

Table 5-319 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.9.3 Modifying an Excluded Request Throttling Configuration

Function

This API is used to modify an excluded configuration of a request throttling policy.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-320 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/throttle-specials/{id}

The following table lists the parameter in the URI.

Table 5-321 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Excluded request throttling configuration ID

Request

Table 5-322 Parameter description

Parameter	Mandatory	Type	Description
call_limits	Yes	Integer	Maximum number of times the excluded object can access an API within the throttling period

Example request:

```
{
  "call_limits": 180
}
```

Response

Table 5-323 Parameter description

Parameter	Type	Description
id	String	Excluded request throttling configuration ID
strategy_id	String	ID of the request throttling policy to which the excluded configuration belongs
instance_id	Integer	ID of an object specified in the excluded request throttling configuration
instance_name	String	Name of an app or a tenant to which the excluded request throttling configuration applies
instance_type	Integer	Type of the excluded object
call_limits	Integer	Maximum number of times the excluded object can access an API within the throttling period

Parameter	Type	Description
apply_time	Timestamp	Time when the excluded request throttling configuration is created
app_id	String	ID of the app to which the excluded request throttling configuration applies
app_name	String	Name of the app to which the excluded request throttling configuration applies

Example response:

```
{
  "id": "778879b8-df10-495b-a087-874859fdea6d",
  "strategy_id": "a3106cfe-801f-4919-b0d7-d785dc5b47f9",
  "instance_id": "98efd77d-10b5-4eca-8170-ed30a4a286a4",
  "instance_name": "app_002",
  "instance_type": "APP",
  "call_limits": 180,
  "apply_time": "2017-12-29T03:11:18Z",
  "app_id": "98efd77d-10b5-4eca-8170-ed30a4a286a4",
  "app_name": "app_002"
}
```

Status Codes

Table 5-324 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.9.4 Deleting an Excluded Request Throttling Configuration

Function

This API is used to delete an excluded configuration of a request throttling policy.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-325 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/throttle-specials/{id}

The following table lists the parameter in the URI.

Table 5-326 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Excluded request throttling configuration ID

Request

N/A

Response

N/A

Status Codes

Table 5-327 Status codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.9.5 Querying the List of Excluded Request Throttling Configurations

Function

This API is used to query all excluded configurations of a request throttling policy.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-328 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/throttle-specials/{strategy_id}[?page_size, page_no, instance_type, app_name, user]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **strategy_id**, **app_name**, **user**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-329 Parameter description

Parameter	Mandatory	Type	Description
strategy_id	Yes	String	Request throttling policy ID
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .
instance_type	No	String	Object type, which can be APP or USER
app_name	No	String	Name of an excluded app
user	No	String	Account ID

Request

N/A

Response

Table 5-330 Parameter description

Parameter	Type	Description
throttle_specials	Dictionary	Excluded request throttling configuration list
total	Integer	Number of excluded request throttling configurations that match the query conditions
size	Integer	Length of the returned excluded request throttling configuration list

Table 5-331 Parameter description of throttle_specials

Parameter	Type	Description
id	String	Excluded request throttling configuration ID
strategy_id	String	ID of the request throttling policy to which the excluded request throttling configuration belongs
instance_id	Integer	ID of an object specified in the excluded request throttling configuration
instance_name	String	Name of an app or a tenant to which the excluded request throttling configuration applies
instance_type	Integer	Type of the excluded object
call_limits	Integer	Maximum number of times the excluded object can access an API within the throttling period
apply_time	Timestamp	Time when the excluded request throttling configuration is created
app_id	String	ID of the app to which the excluded request throttling configuration applies
app_name	String	Name of the app to which the excluded request throttling configuration applies

Example response:

```
{
  "total": 1,
  "size": 1,
  "throttle_specials": [{
    "id": "778879b8-df10-495b-a087-874859fdea6d",
    "strategy_id": "a3106cfe-801f-4919-b0d7-d785dc5b47f9",
```

```
{
  "instance_id": "98efd77d-10b5-4eca-8170-ed30a4a286a4",
  "instance_name": "app_002",
  "instance_type": "APP",
  "call_limits": 180,
  "apply_time": "2017-12-29T03:11:18Z",
  "app_id": "98efd77d-10b5-4eca-8170-ed30a4a286a4",
  "app_name": "app_002"
}
```

Status Codes

Table 5-332 Status codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.10 Access Control Policy Management

5.10.1 Object Model

To improve access security of a published API, you can control the access from certain IP addresses by configuring a blacklist or whitelist. This section describes the object model for blacklist/whitelist (access control policy) management, as shown in [object model for access control policies](#).

NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of C is mandatory.

Table 5-333 Object model for access control policies

Parameter	Type	Description	Operation Type	Mandatory
id	String	Blacklist or whitelist ID	R	-
acl_name	String	Blacklist or whitelist name	CRU	Yes

Parameter	Type	Description	Operation Type	Mandatory
entity_type	String	Object type, which can be: • IP • DOMAIN: tenant name	CRU	Yes
acl_type	String	Access control type, which can be: • PERMIT (whitelist) • DENY (blacklist)	CRU	Yes
acl_value	String	IP address or tenant name	CRU	Yes
project_id	String	ID of the tenant that creates the access control policy	-	-
update_time	Timestamp	Time when the access control policy was last updated	-	-

5.10.2 Creating an Access Control Policy

Function

This API is used to create an access control policy to allow or deny API access from certain IP addresses or domains. The **acl_value** value of a domain is a tenant name rather than a domain name (such as **www.exampleDomain.com**).

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-334 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/acls

Request

Table 5-335 Parameter description

Parameter	Type	Description
acl_name	String	Name of the access control policy The name of an access control policy consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
acl_type	String	Access control type, which can be: ● PERMIT (whitelist) ● DENY (blacklist)
acl_value	String	One or more objects from which the access will be controlled. Separate multiple objects with commas.
entity_type	String	Object type, which can be: ● IP ● DOMAIN

Example request:

```
{
  "acl_name": "test001",
  "acl_type": "PERMIT",
  "acl_value": "192.168.1.5,192.168.10.0/24,192.168.12.12-192.168.12.19",
  "entity_type": "IP"
}
```

Response

Table 5-336 Parameter description

Parameter	Type	Description
id	String	Access control policy ID
acl_name	String	Access control policy name
acl_type	String	Access control type, which can be: ● PERMIT (whitelist) ● DENY (blacklist)
acl_value	String	Access control objects
entity_type	String	Object type, which can be: ● IP ● DOMAIN

Parameter	Type	Description
update_time	Timestamp	Time when the access control policy was last updated

Example response:

```
{
  "id": "d402b35e-1054-4280-b1c5-0d741a28c995",
  "acl_name": "test",
  "entity_type": "IP",
  "acl_type": "PERMIT",
  "acl_value": "192.168.1.5,192.168.10.0/24,192.168.12.12-192.168.12.19",
  "update_time": "2017-11-18T14:27:36.918578+08:00"
}
```

Status Codes

Table 5-337 Status codes

Status Code	Description
201	Created
400	Bad Request
500	Server Internal Error

5.10.3 Modifying an Access Control Policy

Function

This API is used to modify a specified access control policy. Only attributes **acl_name**, **acl_type**, and **acl_value** can be modified.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-338 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/acls/{id}

The following table lists the parameter in the URI.

Table 5-339 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the access control policy that you want to modify. Obtain the ID by querying the access control policy.

Request

Table 5-340 Parameter description

Parameter	Type	Description
acl_name	String	Name of the access control policy The name of an access control policy consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
acl_type	String	Access control type, which can be: ● PERMIT (whitelist) ● DENY (blacklist)
acl_value	String	One or more objects from which the access will be controlled. Separate multiple objects with commas.

Example request:

```
{
  "acl_name": "string",
  "acl_type": "PERMIT",
  "acl_value": "19asdfaf-adfadf"
}
```

Response

Table 5-341 Parameter description

Name	Type	Description
id	String	Access control policy ID
acl_name	String	Access control policy name
acl_type	String	Access control type, which can be: ● PERMIT (whitelist) ● DENY (blacklist)

Name	Type	Description
acl_value	String	Access control objects
update_time	Timestamp	Time when the access control policy was last updated

Example response:

```
{
  "id": "d402b35e-1054-4280-b1c5-0d741a28c995",
  "acl_name": "goodone",

  "acl_type": "PERMIT",
  "acl_value": "19asdfaf-adfadf",
  "update_time": "2017-11-18T14:27:36.918578+08:00"
}
```

Status Codes

Table 5-342 Status codes

Status Code	Description
200	OK
400	Bad Request
403	Forbidden
404	Not Found

5.10.4 Deleting an Access Control Policy

Function

This API is used to delete a specified access control policy. Access control policies bound to APIs cannot be deleted.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-343 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/acls/{id}

The following table lists the parameter in the URI.

Table 5-344 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Access control policy ID

Request

N/A

Response

N/A

Status Codes

Table 5-345 Status codes

Status Code	Description
204	No Content
403	Forbidden
404	Not Found
500	Server Internal Error

5.10.5 Deleting Multiple Access Control Policies

Function

This API is used to delete multiple access control policies.

Access control policies bound to APIs cannot be deleted.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-346 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/acls[?action]

The following table lists the parameter in the URI.

Table 5-347 Parameter description

Parameter	Mandatory	Type	Description
action	Yes	String	The value must be delete .

Request

Table 5-348 Parameter description

Parameter	Mandatory	Type	Description
acls	No	String Array	IDs of the access control policies to be deleted

Example request:

```
{
  "acls": ["81efcfd94b8747a0b21e8c04144a4e8c", "7addcd00cfab433984b1d8bf2fe08aaa"]
}
```

Response

Table 5-349 Parameter description

Parameter	Type	Description
success_count	Number	Number of successfully deleted access control policies
failure	Array	Error message and access control policies that fail to be deleted

Table 5-350 Parameter description of failure

Parameter	Type	Description
acl_id	String	ID of an access control policy that fails to be deleted
acl_name	String	Name of the access control policy
error_code	String	Error code
error_msg	String	Error message

Example response:

```
{
  "failure": [{
    "ac_id": "81efcd94b8747a0b21e8c04144a4e8c",
    "acl_name": "acl1",
    "error_code": "APIG.3447",
    "error_msg": "The Acl Strategy has already binded to APIs"
  }],
  "success_count": 3
}
```

Status Codes

Table 5-351 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.10.6 Querying Details of an Access Control Policy

Function

This API is used to query the details of a specified access control policy.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-352 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/acls/{id}

The following table lists the parameter in the URI.

Table 5-353 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Access control policy ID

Request

N/A

Response

Table 5-354 Parameter description

Parameter	Type	Description
id	String	Access control policy ID
acl_name	String	Access control policy name
acl_type	String	Access control type, which can be: ● PERMIT (whitelist) ● DENY (blacklist)
acl_value	String	Access control objects
entity_type	String	Object type, which can be: ● IP ● DOMAIN
update_time	Timestamp	Time when the access control policy was last updated

Example response:

```
{
  "id": "d402b35e-1054-4280-b1c5-0d741a28c995",
  "acl_name": "goodone",
  "entity_type": "DOMAIN",
  "acl_type": "PERMIT",
  "acl_value": "19asdfaf-adfadf",
  "update_time": "2017-11-18T14:27:36.918578+08:00"
}
```

Status Codes

Table 5-355 Status codes

Status Code	Description
200	OK
400	Bad Request
403	Forbidden
404	Not Found

5.10.7 Querying the Access Control Policy List

Function

This API is used to query the list of all access control policies.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-356 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/acls[?page_size, page_no, id, name, acl_type, entity_type]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **id**, **name**, **acl_type**, **entity_type**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-357 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Access control policy ID
name	No	String	Access control policy name
acl_type	No	String	Access control type, which can be PERMIT or DENY

Parameter	Mandatory	Type	Description
entity_type	No	String	Object type, which can be IP or DOMAIN
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .
precise_search	No	String	Parameter name (name) for exact matching

Request

N/A

Response

Table 5-358 Parameter description

Parameter	Type	Description
size	Integer	Number of access control policies displayed on the current page
total	Integer	Total number of access control policies
acls	Dictionary	Access control policy list

Table 5-359 Parameter description of acls

Parameter	Type	Description
id	String	Access control policy ID
acl_name	String	Access control policy name
acl_type	String	Access control type, which can be: ● PERMIT (whitelist) ● DENY (blacklist)
acl_value	String	Access control objects
entity_type	String	Object type, which can be: ● IP ● DOMAIN

Parameter	Type	Description
update_time	Timestamp	Time when the access control policy was last updated
bind_num	Integer	Number of APIs to which the access control policy has been bound

Example response:

```
{
  "total": 1,
  "size": 1,
  "acls": [{
    "id": "d402b35e-1054-4280-b1c5-0d741a28c995",
    "acl_name": "goodone",
    "entity_type": "DOMAIN",
    "acl_type": "PERMIT",
    "acl_value": "19asdfaf-adfadf",
    "update_time": "2017-11-18T14:27:36.918578+08:00",
    "bind_num": 1
  }]
}
```

Status Codes

Table 5-360 Status codes

Status Code	Description
200	OK
400	Bad Request
500	Server Internal Error

5.11 Binding Access Control Policies

5.11.1 Object Model

An access control policy can protect access security of an API only after being bound to the API. This section describes the object model for binding an access control policy to an API, as shown in [Table 5-361](#).

NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of C is mandatory.

Table 5-361 Object model for binding an access control policy

Parameter	Type	Description	Operation Type	Mandatory
id	String	Binding ID	R	-
front_api_id	String	API ID	CR	Yes
env_id	String	Environment ID	CR	Yes
acl_id	String	Access control policy ID	CR	Yes
create_time	Timestamp	Time when the access control policy is bound to the API	CR	No

5.11.2 Binding an Access Control Policy to an API

Function

This API is used to bind an access control policy to a specified API.

You can bind different access control policies to an API in different environments, but you can bind only one type of access control policy to the API in each environment.

URI

The following table lists the HTTPS request method and URI of the API.

Table 5-362 HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/acl-bindings

Request

Table 5-363 Parameter description

Parameter	Type	Description
acl_id	String	Access control policy ID
publish_ids	[]String	API publication record ID

Example request:

```
{
  "acl_id": "206bb985d8a04ec09f13c3e51ef77095",
  "publish_ids": [
    "1bc8b2b741a04bd4af3ef9d7cd003104"
  ]
}
```

Response

Table 5-364 Parameter description

Parameter	Type	Description
id	String	Binding ID
api_id	String	API ID
env_id	String	Environment ID
acl_id	String	Access control policy ID
create_time	Timestamp	Time when the access control policy is bound to the API

Example response:

```
[
  {
    "id": "4ffc0da71ddd4c22add8ff801e19846c",
    "api_id": "aebacac6095942b4b2dd2b209bb7b9bc",
    "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
    "acl_id": "206bb985d8a04ec09f13c3e51ef77095",
    "create_time": "2018-07-27T11:27:10.7470224Z"
  }
]
```

Status Codes

Table 5-365 Status codes

Status Code	Description
201	Created
400	Bad Request
403	Forbidden
404	Not Found
500	Server Internal Error

5.11.3 Querying the List of Access Control Policies Bound to an API

Function

This API is used to query the list of access control policies that have been bound to a specified API.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-366 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/acl-bindings/binded-acls[?page_no,page_size,api_id,env_id,env_name,acl_id,acl_name]

 NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **api_id**, **env_id**, **env_name**, **acl_id**, **acl_name**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-367 Parameter description

Parameter	Mandatory	Type	Description
api_id	Yes	String	API ID
env_id	No	String	Environment ID
env_name	No	String	Environment name
acl_id	No	String	Access control policy ID
acl_name	No	String	Access control policy name
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .

Parameter	Mandatory	Type	Description
page_no	No	Integer	Page number. The default value is 1.

Request

N/A

Response

Table 5-368 Parameter description

Parameter	Type	Description
total	Integer	Number of access control policies bound to the API
size	Integer	Number of returned access control policies
acls	Dictionary	Access control policy list

Table 5-369 Parameter description of acls

Parameter	Type	Description
acl_id	String	Access control policy ID
acl_name	String	Access control policy name
acl_type	String	Access control type, which can be: ● PERMIT (whitelist) ● DENY (blacklist)
acl_value	String	Access control objects
entity_type	String	Object type, which can be: ● IP ● DOMAIN ● ADMIN
env_id	String	ID of the environment in which the access control policy takes effect
env_name	String	Name of the environment in which the access control policy takes effect
bind_id	String	Binding ID

Parameter	Type	Description
bind_time	Timestamp	Time when the access control policy is bound to the API

Example response:

```
{
  "total": 1,
  "size": 1,
  "acls": [
    {
      "acl_id": "206bb985d8a04ec09f13c3e51ef77095",
      "acl_name": "acl_001",
      "entity_type": "IP",
      "acl_type": "PERMIT",
      "acl_value": "192.168.1.14,192.168.2.0/24,192.168.1.8-192.168.1.110",
      "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
      "env_name": "RELEASE",
      "bind_id": "4ffc0da71ddd4c22add8ff801e19846c",
      "bind_time": "2018-07-27T11:27:10Z"
    }
  ]
}
```

Status Codes

Table 5-370 Status codes

Status Code	Description
200	OK
400	Bad Request
403	Forbidden
404	Not Found
500	Server Internal Error

5.11.4 Querying the List of APIs Bound to an Access Control Policy

Function

This API is used to query the list of APIs bound to a specified access control policy.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-371 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/acl-bindings/binded-apis[?page_no,page_size,acl_id,env_id,api_id,api_name,group_id]

 NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **acl_id**, **api_id**, **api_name**, **group_id**, **env_id**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-372 Parameter description

Parameter	Mandatory	Type	Description
acl_id	Yes	String	Access control policy ID
api_id	No	String	API ID
api_name	No	String	API name
group_id	No	String	API group ID
env_id	No	String	Environment ID
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .

Request

N/A

Response

Table 5-373 Parameter description

Parameter	Type	Description
total	Integer	Number of APIs to which the access control policy has been bound
size	Integer	Number of returned APIs
apis	Dictionary	API list

Table 5-374 Parameter description of apis

Parameter	Type	Description
api_id	String	API ID
api_name	String	API name
group_name	String	API group name
api_type	Integer	API type
api_remark	String	Description of the API
env_id	String	ID of the environment in which the access control policy takes effect
env_name	String	Name of the environment in which the access control policy takes effect
bind_id	String	Binding ID
bind_time	Timestamp	Time when the access control policy is bound to the API
publish_id	String	ID of the API publication record

Example response:

```
{
  "total": 1,
  "size": 1,
  "apis": [
    {
      "api_id": "aebacac6095942b4b2dd2b209bb7b9bc",
      "api_name": "aaa",
      "group_name": "test001",
      "api_type": 1,
      "api_remark": "aaa",
      "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
      "env_name": "RELEASE",
      "bind_id": "4ffc0da71ddd4c22add8ff801e19846c",
      "bind_time": "2018-07-27T11:27:10Z",
      "publish_id": "1bc8b2b741a04bd4af3ef9d7cd003104"
    }
  ]
}
```

```
}  
  ]  
}
```

Status Codes

Table 5-375 Status codes

Status Code	Description
200	OK
400	Bad Request
403	Forbidden
404	Not Found
500	Server Internal Error

5.11.5 Querying the List of APIs Not Bound to an Access Control Policy

Function

This API is used to query the list of published APIs that have not been bound to a specified access control policy.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-376 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/acl-bindings/unbinded-apis[?page_no,page_size,acl_id,env_id,api_id,api_name,group-id]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **acl_id**, **env_id**, **api_id**, **group_id**, **api_name**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-377 Parameter description

Parameter	Mandatory	Type	Description
acl_id	Yes	String	Access control policy ID
env_id	No	String	Environment ID
group_id	No	String	API group ID
api_id	No	String	API ID
api_name	No	String	API name
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .

Request

N/A

Response

Table 5-378 Parameter description

Parameter	Type	Description
total	Integer	Number of APIs that match the query conditions
size	Integer	Number of returned APIs
apis	Dictionary	API list

Table 5-379 Parameter description of apis

Parameter	Type	Description
id	String	API ID
name	String	API name
group_id	String	ID of the API group to which the API belongs
group_name	String	Name of the API group to which the API belongs

Parameter	Type	Description
type	Integer	Opening status of the API
remark	String	Description of the API
run_env_name	String	Name of the environment in which the API has been published
run_env_id	String	ID of the environment in which the API has been published
publish_id	String	ID of the API publication record
acl_name	String	Name of the same type of access control policy that has been bound to the API
req_uri	String	Access address
auth_type	String	Security authentication mode

Example response:

```
{
  "total": 1,
  "size": 1,
  "apis": [
    {
      "name": "bbbbbb",
      "type": 1,
      "remark": "aaa",
      "group_id": "70f1b578da9b4dfe889b4c33d1b995c2",
      "id": "91c26288acea4448be205265d77dae22",
      "group_name": "test001",
      "run_env_name": "RELEASE",
      "run_env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
      "publish_id": "a6e06a00c382436eb524fa2dd343cb6d",
      "req_uri": "/test",
      "auth_type": "NONE"
    }
  ]
}
```

Status Codes

Table 5-380 Status codes

Status Code	Description
200	OK
400	Bad Request
403	Forbidden
404	Not Found
500	Server Internal Error

5.11.6 Unbinding an Access Control Policy from an API

Function

This API is used to unbind an access control policy from an API.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-381 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/acl-bindings/{id}

The following table lists the parameter in the URI.

Table 5-382 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Binding ID

Request

N/A

Response

N/A

Status Codes

Table 5-383 Status codes

Status Code	Description
204	No Content
403	Forbidden
404	Not Found
500	Server Internal Error

5.11.7 Unbinding Multiple Access Control Policies from APIs

Function

This API is used to unbind multiple access control policies from APIs.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-384 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/acl-bindings[?action]

The following table lists the parameter in the URI.

Table 5-385 Parameter description

Parameter	Mandatory	Type	Description
action	Yes	String	The value must be delete .

Request

Table 5-386 Parameter description

Parameter	Mandatory	Type	Description
acl_bindings	No	String Array	IDs of the access control policies to be unbound

Example request:

```
{
  "acl_bindings": ["81efcd94b8747a0b21e8c04144a4e8c", "7addcd00cfab433984b1d8bf2fe08aaa"]
}
```


Response

Table 5-387 Parameter description

Parameter	Type	Description
success_count	Number	Number of successfully unbound access control policies
failure	Array	Error message and access control policies that fail to be unbound

Table 5-388 Parameter description of failure

Parameter	Type	Description
bind_id	String	ID of an access control policy that fails to be unbound
error_code	String	Error code
error_msg	String	Error message
api_id	String	ID of an API from which an access control policy fails to be unbound
api_name	String	Name of the API from which an access control policy fails to be unbound

Example response:

```
{
  "failure": [{
    "bind_id": "81efcf94b8747a0b21e8c04144a4e8c",
    "error_code": "APIG.3010",
    "error_msg": "Access control policy binding record not found",
    "api_id": "81efcf94b8747a0b21e8c04144a4e8c",
    "api_name": "api01"
  }],
  "success_count": 3
}
```

Status Codes

Table 5-389 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Server Internal Error

5.12 Querying Subscription Information in KooGallery

5.12.1 Querying the List of Purchased API Groups

Function

This API is used to query the list of purchased API groups.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-390 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/purchases/groups[?page_size, page_no, id, group_id, group_name]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **id**, **group_id**, **group_name**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-391 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Subscription ID
group_id	No	String	API group ID
group_name	No	String	API group name
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .

Parameter	Mandatory	Type	Description
page_no	No	Integer	Page number. The default value is 1.

Request

N/A

Response

Table 5-392 Parameter description

Parameter	Type	Description
total	Integer	Total number of API groups that match the query conditions
size	Integer	Number of returned API groups
purchases	Dictionary	API group list

Table 5-393 Parameter description of purchases

Parameter	Type	Description
id	String	Subscription ID
group_id	String	API group ID
group_name	String	API group name
group_remark	String	Description of the API group
order_time	Timestamp	Time when the order is placed
start_time	Timestamp	Time when the order takes effect
expire_time	Timestamp	Time when the order expires
group_domains	[]String	List of API group domain names. No value will be returned when you query the list of purchased API groups.
quota_left	Integer	Remaining API call quota
quota_used	Integer	Used API call quota
app_key	String	Generated AppKey
app_secret	String	Generated AppSecret

Example response:

```
{
  "total": 3,
  "size": 3,
  "purchases": [{
    "id": "615af8d9-f31d-4cdf-8807-b191dc969a07",
    "group_id": "f0585333-5722-4878-b7fa-31ae00b6ae3a",
    "group_name": "api_group_003",
    "group_remark": "API group 003",
    "group_domains": null,
    "quota_used": 0,
    "quota_left": 2000000000,
    "order_time": "2017-12-29T06:22:46Z",
    "start_time": "2018-01-01T00:00:00Z",
    "expire_time": "2019-01-01T00:00:00Z",
    "app_key": "0e24****4785",
    "app_secret": "*****"
  },
  {
    "id": "9d0b****e4d13",
    "group_id": "02a8****71ae7",
    "group_name": "api_group_002",
    "group_remark": "API group 002",
    "group_domains": null,
    "quota_used": 0,
    "quota_left": 2000000000,
    "order_time": "2017-12-29T06:22:46Z",
    "start_time": "2018-01-01T00:00:00Z",
    "expire_time": "2019-01-01T00:00:00Z",
    "app_key": "0e242****04785",
    "app_secret": "*****"
  },
  {
    "id": "3f30d****c587",
    "group_id": "73c5802****47f09",
    "group_name": "api_group_001",
    "group_remark": "API group 001",
    "group_domains": null,
    "quota_used": 0,
    "quota_left": 2000000000,
    "order_time": "2017-12-29T06:16:03Z",
    "start_time": "2018-01-01T00:00:00Z",
    "expire_time": "2019-01-01T00:00:00Z",
    "app_key": "0e242****4785",
    "app_secret": "*****"
  }
  ]
}
```

Status Codes

Table 5-394 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
500	Server Internal Error

5.12.2 Querying Details of a Purchased API Group

Function

This API is used to query the details of a purchased API group.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-395 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/purchases/groups/{purchase_id}

The following table lists the parameter in the URI.

Table 5-396 Parameter description

Parameter	Mandatory	Type	Description
purchase_id	Yes	String	Subscription ID

Request

N/A

Response

Table 5-397 Parameter description

Parameter	Type	Description
id	String	Subscription ID
group_id	String	API group ID
group_name	String	API group name
group_remark	String	Description of the API group
order_time	Timestamp	Time when the order is placed
start_time	Timestamp	Time when the order takes effect
expire_time	Timestamp	Time when the order expires

Parameter	Type	Description
group_domains	[]String	List of API group domain names. A value will be returned when you query the details of a purchased API group.
quota_left	Integer	Remaining API call quota
quota_used	Integer	Used API call quota
app_key	String	Generated AppKey
app_secret	String	Generated AppSecret

Example response:

```
{
  "id": "3f3****cc587",
  "group_id": "73c58****7f09",
  "group_name": "api_group_001",
  "group_remark": "API group 001",
  "group_domains": [
    "test.market.example.com"
  ],
  "quota_used": 0,
  "quota_left": 2000000000,
  "order_time": "2018-01-02T10: 51: 26Z",
  "start_time": "2018-01-01T00: 00: 00Z",
  "expire_time": "2019-01-01T00: 00: 00Z",
  "app_key": "0e242****4785",
  "app_secret": "*****"
}
```

Status Codes

Table 5-398 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

5.12.3 Querying the List of Purchased APIs

Function

This API is used to query the list of purchased APIs.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-399 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/purchases/apis[?page_size, page_no, api_id, api_name, group_id, group_name]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **api_id**, **api_name**, **group_id**, **group_name**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-400 Parameter description

Parameter	Mandatory	Type	Description
api_id	No	String	API ID
api_name	No	String	API name
group_id	No	String	API group ID
group_name	No	String	API group name
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .

Request

N/A

Response

Table 5-401 Parameter description

Parameter	Type	Description
total	Integer	Total number of APIs that match the query conditions
size	Integer	Number of returned APIs
apis	Dictionary	API list

Table 5-402 Parameter description of apis

Parameter	Type	Description
id	String	API ID
name	String	API name
purchase_id	String	Subscription ID
remark	String	Description of the API
req_uri	String	Access address

Example response:

```
{
  "total": 3,
  "size": 3,
  "apis": [{
    "id": "cb498965-8acf-4c98-bd08-4033ef1fcfb4",
    "name": "Environment_list_query",
    "purchase_id": "730f8a84-c8db-45ba-a6a5-2669ceb08574",
    "remark": "Environment list query",
    "req_uri": "/envs"
  },
  {
    "id": "5bbc47e2-95b0-4a56-904e-a3cdc422f8e9",
    "name": "API_group_list_query",
    "purchase_id": "2ae11f50-3938-4560-8b76-58e89bb3f825",
    "remark": "API group list query",
    "req_uri": "/groups"
  },
  {
    "id": "6632a062-9dcf-4f18-9646-3cabb925a290",
    "name": "API_list_query",
    "purchase_id": "2ae11f50-3938-4560-8b76-58e89bb3f825",
    "remark": "API list query",
    "req_uri": "/apis"
  }
  ]
}
```


Status Codes

Table 5-403 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
500	Server Internal Error

5.13 Configuration Management

5.13.1 Object Model

The tenant can manage and modify the default configurations according to the system running status.

 NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of C is mandatory.

Table 5-404 System configuration object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Configuration ID	R	-
module_name	String	Name of the module to which the configuration belongs	R	-
config_name	String	Configuration name	R	-
config_value	String	Configuration value	RU	-
can_special	Integer	Indicates whether excluded configurations are supported. The value can be: • 1: supported • 2: not supported	R	-
remarks	String	Description of the configuration	R	-

Parameter	Type	Description	Operation Type	Mandatory
update_time	Timestamp	Time when the configuration was last updated	RU	-
match_regexp	String	Rule that the configuration value must meet	R	-
encrypt_flag	Integer	Indicates whether to encrypt the config_value parameter. The value can be: • 1: encrypt • 2: not encrypt	R	-

5.13.2 Querying Configuration Details

Function

This API is used to query the configurations and configuration values of a tenant.

URI

Table 5-405 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/config/project[?page_size, page_no, config_id, config_name]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **config_name**, **config_id**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-406 Parameter description

Parameter	Mandatory	Type	Description
config_name	No	String	Configuration name

Parameter	Mandatory	Type	Description
config_id	No	String	Configuration ID
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .

Request

N/A

Response

Table 5-407 Parameter description

Parameter	Type	Description
total	Integer	Total number of configurations that match the query conditions
size	Integer	Length of the returned configuration list
configs	Dictionary	Configuration list

Table 5-408 Parameter description of configs

Parameter	Type	Description
config_id	String	Configuration ID
config_name	String	Configuration name
config_value	String	Configuration value
remark	String	Description of the configuration
config_time	Timestamp	Time when the configuration is created

Example response:

```
{
  "total": 3,
  "size": 3,
  "configs": [
    {
      "config_id": "1",
      "config_name": "API_NUM_LIMIT",
      "config_value": "300",
```

```
{
  "config_time": "2017-12-29T08: 00: 39.543642Z",
  "remark": "Maximum number of APIs a tenant can create"
},
{
  "config_id": "2",
  "config_name": "APP_NUM_LIMIT",
  "config_value": "30",
  "config_time": "2017-12-29T03: 39: 03.165657Z",
  "remark": "Maximum number of apps a tenant can create"
},
{
  "config_id": "3",
  "config_name": "APIGROUP_NUM_LIMIT",
  "config_value": "30",
  "config_time": "2017-12-29T03: 39: 03.165657Z",
  "remark": "Maximum number of API groups a tenant can create"
}
]
```

Status Codes

Table 5-409 Status codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
500	Server Internal Error

5.14 Resource Query

5.14.1 Querying API Group Quantities

Function

This API is used to query the number of API groups that have been listed and the number of API groups that have not been listed.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-410 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/resources/outline/groups

Request

N/A

Response

Table 5-411 Parameter description

Parameter	Type	Description
offsell_nums	Integer	Number of API groups that have not been listed on KooGallery
onsell_nums	Integer	Number of API groups that have been listed on KooGallery

Example response:

```
{
  "offsell_nums": 1,
  "onsell_nums": 2
}
```

Status Codes

Table 5-412 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Server Internal Error

5.14.2 Querying API Quantities

Function

This API is used to query the number of APIs that have been published in the RELEASE environment and the number of APIs that have not been published.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-413 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/resources/outline/apis

Request

N/A

Response

Table 5-414 Parameter description

Parameter	Type	Description
instance_num	Integer	Total number of APIs
nums_off_release	Integer	Number of APIs that have not been published in the RELEASE environment
nums_on_release	Integer	Number of APIs that have been published in the RELEASE environment

Example response:

```
{
  "instance_num": 3,"nums_off_release": 1,
  "nums_on_release": 2
}
```

Status Codes

Table 5-415 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Server Internal Error

5.14.3 Querying App Quantities

Function

This API is used to query the number of apps that have been authorized to access APIs and the number of apps that have not been authorized to access APIs.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-416 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/resources/outline/apps

Request

N/A

Response

Table 5-417 Parameter description

Parameter	Type	Description
authed_nums	Integer	Number of apps that have been authorized to access APIs
unauthed_nums	Integer	Number of apps that have not been authorized to access APIs

Example response:

```
{
  "authed_nums": 1,
  "unauthed_nums": 2
}
```

Status Codes

Table 5-418 Status codes

Status Code	Description
200	OK
400	Bad Request

Status Code	Description
401	Unauthorized
403	Forbidden
500	Server Internal Error

5.15 Signature Key Management

5.15.1 Object Model

This section describes the object model for signature key management.

NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of C is mandatory.

Table 5-419 Object model for signature key management

Parameter	Type	Description	Operation Type	Mandatory
id	String	Signature key ID	R	-
name	String	Signature key name	CRU	Yes
sign_key	String	Signature key	CRU	Yes
sign_secret	String	Signature secret	CRU	Yes
create_time	Timestamp	Time when the signature key is created	R	-
update_time	Timestamp	Time when the signature key was last updated	R	-

5.15.2 Creating a Signature Key

Function

It is a good practice to provide a protection mechanism for APIs to ensure access security. For example, authenticating API request sources and denying the access from unauthorized sources.

A signature key is a protection mechanism in case.

Create a signature key and bind it to an API. When requesting the API, APIG uses the signature key to encrypt request parameter data and generate a signature.

The backend service of the API verifies requests by using the signature. Unauthorized requests will be denied to protect the API against attacks from unknown sources.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-420 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/signs

Request

Table 5-421 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	Signature key name The name of a signature key consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
sign_key	No	String	Signature key A signature key consists of 8–32 characters, starting with a letter or digit. Only letters, digits, hyphens (-), and underscores (_) are allowed. A key is automatically generated by the backend if no key is specified.
sign_secret	No	String	Signature secret A signature secret consists of 16–64 characters, starting with a letter or digit. Only letters, digits, and special characters (-_!@#\$\$%) are allowed. A value is automatically generated by the backend if no value is specified.

Example request:

```
{
  "name": "signature01",
  "sign_key": "abcd_123",
  "sign_secret": "*****"
}
```

Response

Table 5-422 Parameter description

Parameter	Type	Description
id	String	Signature key ID
name	String	Signature key name
sign_key	String	Signature key
sign_secret	String	Signature secret
create_time	Timestamp	Time when the signature key is created
update_time	Timestamp	Time when the signature key was last updated

Example response:

```
{
  "name": "signature01",
  "sign_key": "abcd_123",
  "sign_secret": "*****",
  "id": "3a793b65a9034bdfae08924f149bfb4a",
  "create_time": "2018-02-06T12:17:36.039953112Z",
  "update_time": "2018-02-06T12:17:36.039954198Z"
}
```

Status Codes

Table 5-423 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
500	Server Internal Error

5.15.3 Modifying a Signature Key

Function

This API is used to modify the information about a signature key.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-424 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/signs/{id}

The following table lists the parameter in the URI.

Table 5-425 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Signature key ID

Request

Table 5-426 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	Signature key name The name of a signature key consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
sign_key	No	String	Signature key A signature key consists of 8–32 characters, starting with a letter or digit. Only letters, digits, hyphens (-), and underscores (_) are allowed. A key is automatically generated by the backend if no key is specified.
sign_secret	No	String	Signature secret A signature secret consists of 16–64 characters, starting with a letter or digit. Only letters, digits, and special characters (-_!@\$%) are allowed. A value is automatically generated by the backend if no value is specified.

Example request:

```
{
  "name": "signature01",
  "sign_key": "abcd_1234",
  "sign_secret": "*****"
}
```

Response

Table 5-427 Parameter description

Parameter	Type	Description
id	String	Signature key ID
name	String	Signature key name
sign_key	String	Signature key
sign_secret	String	Signature secret
create_time	Timestamp	Time when the signature key is created
update_time	Timestamp	Time when the signature key was last updated

Example response:

```
{
  "name": "signature01",
  "sign_key": "abcd_123",
  "sign_secret": "*****",
  "id": "3a793b65a9034bdfae08924f149bfb4a",
  "create_time": "2018-02-06T12:17:36.039953112Z",
  "update_time": "2018-02-06T12:17:36.039954198Z"
}
```

Status Codes

Table 5-428 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.15.4 Deleting a Signature Key

Function

This API is used to delete a specified signature key.

This operation will invalidate the signature key and unbind it from relevant APIs.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-429 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/signs/{id}

The following table lists the parameter in the URI.

Table 5-430 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Signature key ID

Request

N/A

Response

N/A

Status Codes

Table 5-431 Status codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.15.5 Querying the Signature Key List

Function

This API is used to query the information about all signature keys.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-432 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/signs[?page_size, page_no, id, name]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **id** and **name**.

Request

Table 5-433 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Signature key ID
name	No	String	Signature key name
precise_search	No	String	Parameter name (name) for exact matching

Response

Table 5-434 Parameter description

Parameter	Type	Description
total	Integer	Number of signature keys that match the query conditions
size	Integer	Length of the returned signature key list
signs	Dictionary	Signature key list

Table 5-435 Parameter description of signs

Parameter	Type	Description
id	String	Signature key ID
name	String	Signature key name
sign_key	String	Signature key
sign_secret	String	Signature secret
create_time	Timestamp	Time when the signature key is created
update_time	Timestamp	Time when the signature key was last updated
bind_num	Integer	Number of APIs to which the signature key has been bound

Example response:

```
{
  "total": 2,
  "size": 2,
  "signs": [{
    "name": "signature01",
    "sign_key": "abcd_1234",
    "sign_secret": "*****",
    "id": "3a793b65a9034bdfae08924f149bfb4a",
    "create_time": "2018-02-06T12:17:36Z",
    "update_time": "2018-02-07T02:00:27.964766Z",
    "bind_num":1
  },
  {
    "name": "sada",
    "sign_key": "asdasdasdasda",
    "sign_secret": "*****",
    "id": "51ce490901f4411fa54eb06d33bd7218",
    "create_time": "2018-02-06T11:53:08Z",
    "update_time": "2018-02-06T11:53:08Z",
    "bind_num":1
  }
  ]
}
```

Status Codes

Table 5-436 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
500	Server Internal Error

5.16 Binding Signature Keys

5.16.1 Object Model

This section describes the object model for binding a signature key to an API.

 NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of C is mandatory.

Table 5-437 Object model for binding a signature key to an API

Parameter	Type	Description	Operation Type	Mandatory
id	String	Binding ID	R	-
front_api_id	String	API ID	CR	Yes
sign_id	String	Signature key ID	CR	Yes
env_id	String	Environment ID	CR	Yes
create_time	Timestamp	Time when the signature key is bound to the API	R	No

5.16.2 Querying the List of APIs Not Bound to a Signature Key

Function

This API is used to query the list of APIs that have not been bound to a specified signature key. Only published APIs will be displayed.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-438 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/sign-bindings/unbound-apis[?page_size, page_no, sign_id, env_id, api_id, api_name, group_id]

 NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **sign_id**, **env_id**, **api_id**, **api_name**, **group_id**, **page_size**, and **page_no**.

Request

Table 5-439 Parameter description

Parameter	Mandatory	Type	Description
sign_id	Yes	String	Signature key ID
env_id	No	String	Environment ID
api_id	No	String	API ID
api_name	No	String	API name
group_id	No	String	API group ID

Response

Table 5-440 Parameter description

Parameter	Type	Description
total	Integer	Total number of APIs that match the query conditions
size	Integer	Length of the returned API list
apis	Dictionary	API list

Table 5-441 Parameter description of apis

Parameter	Type	Description
id	String	API ID
name	String	API name
type	Integer	API type
remark	String	Description of the API
group_id	String	ID of the API group to which the API belongs
group_name	String	Name of the API group to which the API belongs

Parameter	Type	Description
run_env_name	String	Name of the environment in which the API has been published
run_env_id	String	ID of the environment in which the API has been published
publish_id	String	API publication record ID
signature_name	String	Name of the signature key bound to the API
auth_type	String	Security authentication mode
req_uri	String	Access address

Example response:

```
{
  "total": 2,
  "size": 2,
  "apis": [{
    "name": "bbb",
    "type": 1,
    "group_id": "7ccc0b94-eb5a-48e6-8554-6d0105a540e2",
    "id": "3c6769c6-ec61-4b45-b478-c60310dbaa1b",
    "group_name": "asd",
    "run_env_name": "das",
    "run_env_id": "1fdb2e4-f90a-4159-817d-98c9b8e8b215",
    "publish_id": "6dff16c4-813f-486a-bba4-fdad45a55a70",
    "auth_type": "NONE",
    "req_uri": "/test"
  },
  {
    "name": "aaa",
    "type": 1,
    "group_id": "7ccc0b94-eb5a-48e6-8554-6d0105a540e2",
    "id": "d85c502a-f916-47e8-bba0-50537a2d1af2",
    "group_name": "asd",
    "run_env_name": "das",
    "run_env_id": "1fdb2e4-f90a-4159-817d-98c9b8e8b215",
    "publish_id": "dec83400-a0c6-4ea6-abfd-5bf237292f4d",
    "auth_type": "NONE",
    "req_uri": "/test"
  }
  ]
}
```

Status Codes

Table 5-442 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized

Status Code	Description
403	Forbidden
404	Not Found
500	Server Internal Error

5.16.3 Binding a Signature Key

Function

A signature key takes effect only after being bound to an API. When requesting the backend service, APIG uses the signature key to cryptographically sign requests. The backend service verifies the signature to identify request sources.

This API is used to bind a signature key to one or more published APIs.

Different signature keys can be bound to an API in different environments, but only one signature key can be bound to the API in the same environment.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-443 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/sign-bindings

Request

Table 5-444 Parameter description

Parameter	Mandatory	Type	Description
sign_id	Yes	String	Signature key ID
publish_ids	Yes	Array of strings	API publication record ID

Example request:

```
{
  "sign_id": "3a793b65a9034bdfae08924f149bfb4a",
  "publish_ids": [
    "374a6d5a-20c7-4ea1-82e1-19fce4556956",
    "65e6fe53-1ac3-4481-ba36-9f0bc6f22057"
  ]
}
```

```
]
}
```

Response

Table 5-445 Parameter description

Parameter	Type	Description
-	Dictionary	List of APIs bound to the signature key

Table 5-446 Parameter description of the API list

Parameter	Type	Description
id	String	Binding ID
api_id	String	API ID
api_name	String	API name
api_remark	String	Description of the API
group_name	String	Name of the API group to which the API belongs
api_type	Integer	API type
sign_id	String	Signature key ID
sign_name	String	Signature key name
sign_key	String	Signature key
sign_secret	String	Signature secret
env_id	String	ID of the environment in which the API has been published
env_name	String	Name of the environment in which the API has been published
binding_time	Timestamp	Time when the signature key is bound to the API
publish_id	String	ID of the publication record

Example response:

```
[
{
  "id": "d8426fb090e442c4a56a35e451bea085",
  "api_id": "3c6769c6-ec61-4b45-b478-c60310dbaa1b",
  "api_name": "bbb",
  "api_remark": "",
  "group_name": "asd",
  "api_type": 1,
```

```
"sign_id": "3a793b65a9034bdfae08924f149bfb4a",
"sign_name": "signature01",
"sign_key": "abcd_1234",
"sign_secret": "*****",
"env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
"env_name": "RELEASE",
"binding_time": "2018-02-07T03:17:26.396039456Z",
"publish_id": "23234202f5834ab69113fc1b790b6bed"
},
{
  "id": "97952732e6d7452d99de02db99acce27",
  "api_id": "d85c502a-f916-47e8-bba0-50537a2d1af2",
  "api_name": "aaa",
  "api_remark": "",
  "group_name": "asd",
  "api_type": 1,
  "sign_id": "3a793b65a9034bdfae08924f149bfb4a",
  "sign_name": "signature01",
  "sign_key": "abcd_1234",
  "sign_secret": "*****",
  "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "env_name": "RELEASE",
  "binding_time": "2018-02-07T03:17:26.39803282Z",
  "publish_id": "6581f68efddc4ff0815e156ec6ecfb52"
}
]
```

Status Codes

Table 5-447 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.16.4 Querying the List of APIs Bound to a Signature Key

Function

This API is used to query the list of APIs that have been bound to a specified signature key.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-448 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/sign-bindings/binded-apis[?page_size, page_no, sign_id, env_id, api_id, api_name, group_id]

 NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **sign_id**, **env_id**, **api_id**, **api_name**, **group_id**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-449 Parameter description

Parameter	Mandatory	Type	Description
sign_id	Yes	String	Signature key ID
env_id	No	String	Environment ID
api_id	No	String	API ID
api_name	No	String	API name
group_id	No	String	API group ID

Request

N/A

Response

Table 5-450 Parameter description

Parameter	Type	Description
total	Integer	Total number of APIs that match the query conditions
size	Integer	Length of the returned API list
bindings	Dictionary	API list

Table 5-451 Parameter description of bindings

Parameter	Type	Description
id	String	Binding ID
api_id	String	API ID
api_name	String	API name
api_remark	String	Description of the API
group_name	String	Name of the API group to which the API belongs
api_type	Integer	API type
sign_id	String	Signature key ID
sign_name	String	Signature key name
sign_key	String	Signature key
sign_secret	String	Signature secret
env_id	String	ID of the environment in which the API has been published
env_name	String	Name of the environment in which the API has been published
binding_time	Timestamp	Time when the signature key is bound to the API
publish_id	String	API publication ID

Example response:

```
{
  "total": 2,
  "size": 2,
  "bindings": [
    {
      "id": "4588ec6f5dab4f67b298dc693f58029e",
      "api_id": "d85c502a-f916-47e8-bba0-50537a2d1af2",
      "api_name": "aaa",
      "api_remark": "",
      "group_name": "asd",
      "api_type": 1,
      "sign_id": "3a793b65a9034bdfae08924f149bfb4a",
      "sign_name": "signature01",
      "sign_key": "abcd_1234",
      "sign_secret": "*****",
      "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
      "env_name": "RELEASE",
      "binding_time": "2018-02-07T07:08:51Z",
      "publish_id": "3a793b65a9034bdfae08924f149bfdsda"
    },
    {
      "id": "d8426fb090e442c4a56a35e451bea085",
      "api_id": "3c6769c6-ec61-4b45-b478-c60310dbaa1b",
      "api_name": "bbb",
      "api_remark": ""
    }
  ]
}
```

```
{
  "group_name": "asd",
  "api_type": 1,
  "sign_id": "3a793b65a9034bdfae08924f149bfb4a",
  "sign_name": "signature01",
  "sign_key": "abcd_1234",
  "sign_secret": "*****",
  "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
  "env_name": "RELEASE",
  "binding_time": "2018-02-07T03:17:26Z",
  "publish_id": "3a793b65a9034bdfae08924f149bfdsda"
}
```

Status Codes

Table 5-452 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.16.5 Querying the List of Signature Keys Bound to an API

Function

This API is used to query the list of signature keys that have been bound to a specified API. Only one signature key can be bound to an API in an environment.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-453 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/sign-bindings/binded-signs[?page_no, page_size, api_id, sign_id, sign_name, env_id]

 NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **api_id**, **sign_id**, **sign_name**, **env_id**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-454 Parameter description

Parameter	Mandatory	Type	Description
api_id	Yes	String	API ID
sign_id	No	String	Signature key ID
sign_name	No	String	Signature key name
env_id	No	String	Environment ID

Request

N/A

Response

Table 5-455 Parameter description

Parameter	Type	Description
total	Integer	Total number of signature keys that match the query conditions
size	Integer	Length of the returned signature key list
bindings	Dictionary	Signature key list

Table 5-456 Parameter description of bindings

Parameter	Type	Description
id	String	Binding ID
api_id	String	API ID
api_name	String	API name
api_remark	String	Description of the API
group_name	String	Name of the API group to which the API belongs
api_type	Integer	API type

Parameter	Type	Description
sign_id	String	Signature key ID
sign_name	String	Signature key name
sign_key	String	Signature key
sign_secret	String	Signature secret
env_id	String	ID of the environment in which the API has been published
env_name	String	Name of the environment in which the API has been published
binding_time	Timestamp	Time when the signature key is bound to the API
publish_id	String	API publication ID

Example response:

```
{
  "total": 2,
  "size": 2,
  "bindings": [
    {
      "id": "4588ec6f5dab4f67b298dc693f58029e",
      "api_id": "d85c502a-f916-47e8-bba0-50537a2d1af2",
      "api_name": "aaa",
      "api_remark": "",
      "group_name": "asd",
      "api_type": 1,
      "sign_id": "3a793b65a9034bdfae08924f149bfb4a",
      "sign_name": "signature01",
      "sign_key": "abcd_1234",
      "sign_secret": "*****",
      "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
      "env_name": "RELEASE",
      "binding_time": "2018-02-07T07: 08: 51Z",
      "publish_id": "3a793b65a9034bdfae08924f149bfsda"
    },
    {
      "id": "d8426fb090e442c4a56a35e451bea085",
      "api_id": "3c6769c6-ec61-4b45-b478-c60310dbaa1b",
      "api_name": "bbb",
      "api_remark": "",
      "group_name": "asd",
      "api_type": 1,
      "sign_id": "3a793b65a9034bdfae08924f149bfb4a",
      "sign_name": "signature01",
      "sign_key": "abcd_1234",
      "sign_secret": "*****",
      "env_id": "DEFAULT_ENVIRONMENT_RELEASE_ID",
      "env_name": "RELEASE",
      "binding_time": "2018-02-07T03: 17: 26Z",
      "publish_id": "3a793b65a9034bdfae08924f149bfsda"
    }
  ]
}
```

Status Codes

Table 5-457 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.16.6 Unbinding a Signature Key

Function

This API is used to unbind a signature key from an API.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-458 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/sign-bindings/{id}

The following table lists the parameter in the URI.

Table 5-459 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Binding ID

Request

N/A

Response

N/A

Status Codes

Table 5-460 Status codes

Status Code	Description
204	No Content
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.17 Domain Name Management

5.17.1 Object Model

This section describes the object models for certificates and user-defined domain names.

 NOTE

- **Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- **Mandatory** indicates whether a field with the **Operation Type** of C is mandatory.

Table 5-461 Domain name object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Domain ID	R	-
url_domain	String	Domain name	CR	Yes
cname_status	Integer	CNAME resolution status, which can be: • 1: not resolved • 2: in progress • 3: successful • 4: failed	R	No
ssl_id	String	Certificate ID	R	No
group_id	String	API group ID	CR	Yes

Table 5-462 Certificate object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Certificate ID	R	-
name	String	Certificate name	CRU	Yes
context	String	Content of the certificate	CRU	Yes
private_key	String	Private key of the certificate	CRU	Yes

5.17.2 Binding a Domain Name

Function

Domain names are user-defined, and take effect only after CNAME records are added to point the domain names to subdomain names of API groups. For details, see [Adding a CNAME Record Set](#).

An API group can be bound to a maximum of five domain names. After you bind a domain name to an API group, APIs in the group can be called using the domain name.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-463 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/api-groups/{group_id}/domains

The following table lists the parameter in the URI.

Table 5-464 Parameter description

Parameter	Mandatory	Type	Description
group_id	Yes	String	API group ID

Request

Table 5-465 Parameter description

Parameter	Mandatory	Type	Description
url_domain	Yes	String	Domain name A domain name consists of a maximum of 255 characters and must comply with domain name specifications.

Example request:

```
{
  "url_domain": "www.MyCompany.com"
}
```

Response

Table 5-466 Parameter description

Parameter	Type	Description
id	String	Domain ID
url_domain	String	Domain name
status	Integer	CNAME resolution status, which can be: • 1: not resolved • 2: in progress • 3: successful • 4: failed

Example response:

```
{
  "id": "c5e0d5ba62a34d26ad5c709ae22c1a17",
  "url_domain": "www.MyCompany.com",
  "status": 3
}
```

Status Codes

Table 5-467 Status codes

Status Code	Description
201	Created

Status Code	Description
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.17.3 Unbinding a Domain Name

Function

This API is used to unbind a custom domain name from an API group.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-468 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/api-groups/{group_id}/domains/{id}

The following table lists the parameter in the URI.

Table 5-469 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Domain ID
group_id	Yes	String	API group ID

Request

N/A

Response

N/A

Status Codes

Table 5-470 Status codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.17.4 Adding a Certificate to a Domain Name

Function

When you create an API to be accessed through HTTPS, you must add an SSL certificate to the independent domain name that has been bound to the group the API belongs to.

This API is used to add a certificate to a specific domain name.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-471 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/api-groups/{group_id}/domains/{domain_id}/certificate

The following table lists the parameters in the URI.

Table 5-472 Parameter description

Parameter	Mandatory	Type	Description
group_id	Yes	String	API group ID
domain_id	Yes	String	Domain ID

Request

Table 5-473 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	Certificate name A certificate name consists of 4–50 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
cert_content	Yes	String	Content of the certificate
private_key	Yes	String	Private key

Example request:

```
{
  "cert_content": "example",
  "name": "test_ssl",
  "private_key": "example"
}
```

Response

Table 5-474 Parameter description

Parameter	Type	Description
id	String	Domain ID
url_domain	String	Domain name
status	Integer	CNAME resolution status
ssl_id	String	Certificate ID
ssl_name	String	Certificate name

Example response:

```
{
  "id": " b9be707660c5406394f8973e087bae20",
  "url_domain": "www.example.com",
  "status": 3,
  "ssl_id": "0a515af69f4e4dcca84fbf85f68c0e27",
  "ssl_name": "Certificate"
}
```

Status Codes

Table 5-475 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.17.5 Deleting a Certificate Bound to a Domain Name

Function

This API is used to delete a certificate that is no longer needed or has expired.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-476 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/api-groups/{group_id}/domains/{domain_id}/certificate/{id}

The following table lists the parameter in the URI.

Table 5-477 Parameter description

Parameter	Mandatory	Type	Description
group_id	Yes	String	API group ID
domain_id	Yes	String	Domain ID
id	Yes	String	Certificate ID

Request

N/A

Response

N/A

Status Codes

Table 5-478 Status codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.17.6 Querying Details of a Certificate Bound to a Domain Name

Function

This API is used to query the details of a specified certificate bound to a domain name.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-479 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/api-groups/{group_id}/domains/{domain_id}/certificate/{id}

The following table lists the parameters in the URI.

Table 5-480 Parameter description

Parameter	Mandatory	Type	Description
group_id	Yes	String	API group ID

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Domain ID
id	Yes	String	Certificate ID

Request

N/A

Response

Table 5-481 Parameter description

Parameter	Type	Description
common_name	String	Certificate domain name
san	Dictionary	Subject alternative name (SAN)
version	String	Certificate version
organization	Dictionary	Company or organization
organizational_unit	Dictionary	Department
locality	Dictionary	City
state	Dictionary	Province or state
country	Dictionary	Country or region
not_before	Timestamp	Start time of the certificate validity period
not_after	Timestamp	Expiration time of the certificate validity period
serial_number	String	SN
issuer	Dictionary	Certificate issuer
signature_algorithm	String	Signature algorithm

Example response:

```
{
  "san": [
    "xxx.xxx.xxx"
  ],
  "country": [
    "CN"
  ],
  "not_before": "2019-04-29T11:49:18Z",
```

```
"locality": [
  "XXX"
],
"serial_number": "00000000000000000000000000000000",
"version": 3,
"issuer": [
  "XXX"
],
"not_after": "2029-04-29T11:49:18Z",
"organization": [
  "XXX"
],
"signature_algorithm": "SHA256-RSA",
"state": [
  "XXX"
],
"common_name": "xxx.xxx.xxx",
"organizational_unit": [
  "XXX"
]
}
```

Status Codes

Table 5-482 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.18 VPC Channel Management

5.18.1 Object Model

This section describes the object models for VPC channel management.

NOTE

- Operation Type** indicates the operation that can be performed on a field.
C: create; U: update; R: read
- Mandatory** indicates whether a field with the **Operation Type** of **C** is mandatory.

Table 5-483 VPC channel object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	VPC channel ID	R	-
name	String	VPC channel name	CRU	Yes
type	Integer	VPC channel type, which can be: • 2: built-in channel	CRU	Yes
status	Integer	VPC channel status, which can be: • 1: normal • 2: abnormal	R	Yes
project_id	String	Tenant ID	CRU	Yes
port	Integer	Port number	CR	Yes
balance_strategy	Integer	Distribution algorithm, which can be: • 1: weighted round robin (WRR) • 2: weighted least connection (WLC) • 3: source hashing (SH) • 4: URI hashing	CRU	Yes
create_time	Timestamp	Time when the VPC channel is created	R	Yes

Table 5-484 Health check object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Health check ID	R	-
vpc_id	String	VPC channel ID	CRU	Yes
protocol	String	Protocol for health checks, which can be: • tcp • http	CRU	Yes
path	Integer	Path for health checks, which is valid only when protocol is set to http	CRU	No

Parameter	Type	Description	Operation Type	Mandatory
port	Integer	Port number. The port number of the VPC channel will be used if no value is specified.	CRU	No
threshold_normal	Integer	Healthy threshold	CRU	Yes
threshold_abnormal	Integer	Unhealthy threshold	CRU	Yes
time_out	Integer	Timeout to wait for a response	CRU	Yes
time_interval	Integer	Interval between consecutive checks	CRU	Yes
http_code	String	Success codes, which are valid only when protocol is set to http	CRU	No
create_time	Timestamp	Time when the health check configuration is created	R	Yes

Table 5-485 Backend instance object model

Parameter	Type	Description	Operation Type	Mandatory
id	String	Backend instance object ID	R	-
vpc_id	String	VPC channel ID	CRU	Yes
ext_vpc_id	String	ID of the VPC associated with the backend instance object This parameter is not used currently.	R	Yes
instance_id	String	Instance ID	CRU	No
instance_name	String	Instance name	CRU	No
host	String	IP address of the backend instance object	CRU	Yes

Parameter	Type	Description	Operation Type	Mandatory
status	Integer	Status of the backend instance object 1: normal 2: abnormal	R	Yes
weight	Integer	Weight	CRU	Yes
create_time	Timestamp	Time when the member is created	R	Yes

5.18.2 Creating a VPC Channel

Function

This API is used to create a VPC channel from APIG to your private VPC resources. Afterwards, when creating an API, you can configure your backend service to use this VPC channel so that APIG can directly access your private VPC resources.

NOTE

You can create a maximum of 30 VPC channels.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-486 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/vpc-channels

Request

Table 5-487 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	VPC channel name A VPC channel name consists of 3–64 characters, starting with a letter. Only letters, digits, hyphens (-), and underscores (_) are allowed.

Parameter	Mandatory	Type	Description
type	Yes	Integer	VPC channel type, which can be: • 2: fast channel with the load balancing function
member_type	Mandatory if type is 2	String	Member type of the VPC channel, which can be: • ip (not supported currently) • instance This parameter is valid only when the VPC channel type is set to 2 . The default value is instance .
port	Mandatory if type is 2	Integer	Host port of the VPC channel This parameter is valid only when the VPC channel type is set to 2 . The value range is 1–65535.
balance_strategy	Mandatory if type is 2	Integer	Distribution algorithm, which can be: • 1: WRR • 2: WLC • 3: SH • 4: URI hashing This parameter is valid only when the VPC channel type is set to 2 . The default value is 1 .
vpc_health_config	Mandatory if type is 2	Dictionary	Health check details. This parameter is valid only when the VPC channel type is set to 2 .

Table 5-488 Health check details

Parameter	Mandatory	Type	Description
protocol	Yes	String	Protocol for performing health checks on cloud servers in the VPC channel. The value can be: • TCP • HTTP • HTTPS

Parameter	Mandatory	Type	Description
path	Required when protocol is set to http .	String	Destination path for health checks NOTE The value of this parameter must comply with URI specifications.
port	No	Integer	Destination port for health checks. By default, the host port of the VPC channel is used. Range: 1–65535
threshold_normal	Yes	Integer	Healthy threshold It refers to the number (x) of consecutive successful checks required for a cloud server to be marked as healthy. Range: 2–10
threshold_abnormal	Yes	Integer	Unhealthy threshold It refers to the number (x) of consecutive failed checks required for a cloud server to be marked as unhealthy. Range: 2–10
time_out	Yes	Integer	Timeout for determining whether a health check fails. Unit: s. The value must be less than the value of time_interval . Range: 2–30
time_interval	Yes	Integer	Interval between consecutive checks. Unit: s. The value must be greater than the value of time_out . Range: 5–300
http_code	Required when protocol is set to http .	String	HTTP response codes for determining a successful HTTP response The value can be any integer within 100–599 in one of the following formats: • Multiple values, for example, 200,201,202 • Range, for example, 200-299 • Multiple values and ranges, for example, 201,202,210-299

Table 5-489 Backend instance list

Parameter	Mandatory	Type	Description
instance_name	Yes	String	Backend instance name The name must contain 1–64 characters. Only letters, digits, periods (.), hyphens (-), and underscores (_) are allowed.
instance_id	Yes	String	Backend instance ID The ID must contain 1–64 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
weight	Mandatory if type is 2	Integer	Cloud server weight The larger the weight is, the more requests are forwarded to the backend instance. This parameter is valid only when the VPC channel type is set to 2. The value range is 1–100.

Example request:

```
{
  "balance_strategy": 1,
  "name": "vpc_001",
  "port": 15565,
  "type": 2,
  "member_type": "instance",
  "vpc_health_config": {
    "http_code": "205",
    "path": "/hc",
    "port": 15563,
    "protocol": "http",
    "threshold_abnormal": 5,
    "threshold_normal": 5,
    "time_interval": 200,
    "time_out": 30
  },
  "vpc_instances": [
    {
      "instance_id": "instance01",
      "instance_name": "instance_name01",
      "weight": 10
    }
  ]
}
```

Response

Table 5-490 Parameter description

Parameter	Type	Description
id	String	VPC channel ID

Parameter	Type	Description
name	String	VPC channel name
type	Integer	VPC channel type, which can be: • 2: fast channel with the load balancing function
member_type	String	Member type of the VPC channel, which can be: • ip (not supported currently) • instance This parameter is valid only when the VPC channel type is set to 2.
status	Integer	VPC channel status, which can be: • 1: normal • 2: abnormal
port	Integer	Host port of the VPC channel
balance_strategy	Integer	Distribution algorithm, which can be: • 1: WRR • 2: WLC • 3: SH • 4: URI hashing
create_time	Timestamp	Time when the VPC channel is created

Example response:

```
{
  "name": "vpc_001",
  "type": 2,
  "member_type": "instance",
  "port": 15565,
  "balance_strategy": 1,
  "id": "c3e6a7d85d9e47be89dfcc3cd37405d7",
  "create_time": "2018-07-27T12:30:48.027484Z",
  "status": 1
}
```

Status Codes

Table 5-491 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized

Status Code	Description
403	Forbidden
404	Not Found
500	Server Internal Error

5.18.3 Updating a VPC Channel

Function

This API is used to update the parameters of a specified VPC channel.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-492 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/vpc-channels/{id}

The following table lists the parameter in the URI.

Table 5-493 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	VPC channel ID

Request

Table 5-494 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	VPC channel name A VPC channel name consists of 3–64 characters, starting with a letter. Only letters, digits, hyphens (-), and underscores (_) are allowed.

Parameter	Mandatory	Type	Description
type	Yes	Integer	VPC channel type, which can be: • 2: fast channel with the load balancing function
member_type	Mandatory if type is 2	String	Member type of the VPC channel, which can be: • ip (not supported currently) • instance This parameter is valid only when the VPC channel type is set to 2 . The default value is instance .
port	Mandatory if type is 2	Integer	Host port of the VPC channel This parameter is valid only when the VPC channel type is set to 2 . The value range is 1–65535.
balance_strategy	Mandatory if type is 2	Integer	Distribution algorithm, which can be: • 1: WRR • 2: WLC • 3: SH • 4: URI hashing This parameter is valid only when the VPC channel type is set to 2 . The default value is 1 .
vpc_health_config	Mandatory if type is 2	Dictionary	Health check details. This parameter is valid only when the VPC channel type is set to 2 .
vpc_instances	Yes	Dictionary	Backend instance list. Only one backend instance is included if the VPC channel type is set to 1 .

Table 5-495 Health check details

Parameter	Mandatory	Type	Description
protocol	Yes	String	Protocol for performing health checks on cloud servers in the VPC channel. The value can be: • TCP • HTTP • HTTPS

Parameter	Mandatory	Type	Description
path	Required if protocol is set to http .	String	Destination path for health checks NOTE The value of this parameter must comply with URI specifications.
port	No	Integer	Destination port for health checks. By default, the host port of the VPC channel is used. Range: 1–65535
threshold_normal	Yes	Integer	Healthy threshold It refers to the number (x) of consecutive successful checks required for a cloud server to be marked as healthy. Range: 2–10
threshold_abnormal	Yes	Integer	Unhealthy threshold It refers to the number (x) of consecutive failed checks required for a cloud server to be marked as unhealthy. Range: 2–10
time_out	Yes	Integer	Timeout for determining whether a health check fails. Unit: s. The value must be less than the value of time_interval . Range: 2–30
time_interval	Yes	Integer	Interval between consecutive checks. Unit: s. The value must be greater than the value of time_out . Range: 5–300
http_code	Required if protocol is set to http .	String	HTTP response codes for determining a successful HTTP response The value can be any integer within 100–599 in one of the following formats: • Multiple values, for example, 200,201,202 • Range, for example, 200-299 • Multiple values and ranges, for example, 201,202,210-299

Table 5-496 Backend instance list

Parameter	Mandatory	Type	Description
instance_name	Yes	String	Backend instance name The name must contain 1–64 characters. Only letters, digits, periods (.), hyphens (-), and underscores (_) are allowed.
instance_id	Yes	String	Backend instance ID The ID must contain 1–64 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
weight	Mandatory if type is 2	Integer	Cloud server weight The larger the weight is, the more requests are forwarded to the backend instance. This parameter is valid only when the VPC channel type is set to 2. The value range is 1–100.

Example request:

```
{
  "balance_strategy": 1,
  "name": "vpc_001",
  "port": 15565,
  "type": 2,
  "member_type": "instance",
  "vpc_health_config": {
    "http_code": "205",
    "path": "/hc",
    "port": 15563,
    "protocol": "http",
    "threshold_abnormal": 5,
    "threshold_normal": 5,
    "time_interval": 200,
    "time_out": 30
  },
  "vpc_instances": [
    {
      "instance_id": "instance01",
      "instance_name": "instance_name01",
      "weight": 10
    }
  ]
}
```

Response

Table 5-497 Parameter description

Parameter	Type	Description
id	String	VPC channel ID

Parameter	Type	Description
name	String	VPC channel name
type	Integer	VPC channel type, which can be: 2: fast channel with the load balancing function
member_type	String	Member type of the VPC channel, which can be: - ip (not supported currently) - instance This parameter is valid only when the VPC channel type is set to 2.
status	Integer	VPC channel status, which can be: 1: normal 2: abnormal
port	Integer	Host port of the VPC channel
balance_strategy	Integer	Distribution algorithm, which can be: 1: WRR 2: WLC 3: SH 4: URI hashing
create_time	Timestamp	Time when the VPC channel is created

Example response:

```
{
  "name": "vpc_001",
  "type": 2,
  "member_type": "instance",
  "port": 15565,
  "balance_strategy": 1,
  "id": "c3e6a7d85d9e47be89dfcc3cd37405d7",
  "create_time": "2018-07-27T12:30:48.027484Z",
  "status": 1
}
```

Status Codes

Table 5-498 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized

Status Code	Description
403	Forbidden
404	Not Found
500	Server Internal Error

5.18.4 Deleting a VPC Channel

Function

This API is used to delete a specified VPC channel.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-499 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/vpc-channels/{id}

The following table lists the parameter in the URI.

Table 5-500 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	VPC channel ID

Request

N/A

Response

N/A

Status Codes

Table 5-501 Status codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.18.5 Querying VPC Channel Details

Function

This API is used to query the details of a specified VPC channel.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-502 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/vpc-channels/{id}

The following table lists the parameter in the URI.

Table 5-503 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	VPC channel ID

Request

N/A

Response

Table 5-504 Parameter description

Parameter	Type	Description
id	String	VPC channel ID
name	String	VPC channel name
type	Integer	VPC channel type, which can be: • 2: fast channel with the load balancing function
member_type	String	Member type of the VPC channel, which can be: • ip (not supported currently) • instance
status	Integer	VPC channel status, which can be: • 1: normal • 2: abnormal
port	Integer	Host port of the VPC channel
balance_strategy	Integer	Distribution algorithm, which can be: • 1: WRR • 2: WLC • 3: SH • 4: URI hashing
create_time	Timestamp	Time when the VPC channel is created
vpc_health_config	Dictionary	Health check details
vpc_instances	Dictionary	Backend instance list

Table 5-505 Health check details

Parameter	Type	Description
id	String	Health check ID
vpc_id	String	VPC channel ID
protocol	String	Protocol for performing health checks on cloud servers in the VPC channel. The value can be: • TCP • HTTP • HTTPS

Parameter	Type	Description
path	String	Destination path for health checks NOTE The value of this parameter must comply with URI specifications.
port	Integer	Destination port for health checks. By default, the host port of the VPC channel is used. Range: 1–65535
threshold_normal	Integer	Healthy threshold It refers to the number (x) of consecutive successful checks required for a cloud server to be marked as healthy. Range: 2–10
threshold_abnormal	Integer	Unhealthy threshold It refers to the number (x) of consecutive failed checks required for a cloud server to be marked as unhealthy. Range: 2–10
time_out	Integer	Timeout for determining whether a health check fails. Unit: s. The value must be less than the value of time_interval . Range: 2–30
time_interval	Integer	Interval between consecutive checks. Unit: s. The value must be greater than the value of time_out . Range: 5–300
http_code	String	HTTP response codes for determining a successful HTTP response The value can be any integer within 100–599 in one of the following formats: • Multiple values, for example, 200,201,202 • Range, for example, 200-299 • Multiple values and ranges, for example, 201,202,210-299
create_time	Timestamp	Time when the VPC channel is created

Table 5-506 Backend instance details

Parameter	Type	Description
id	String	Backend instance object ID
vpc_id	String	VPC channel ID

Parameter	Type	Description
status	Integer	Status of the backend instance object
instance_name	String	Backend instance name
instance_id	String	Backend instance ID
host	String	IP address of the backend instance
weight	Integer	Cloud server weight The larger the weight is, the more requests are forwarded to the backend instance. Range: 1–100
create_time	Timestamp	Time when the backend instance is added to the VPC channel

Example response:

```
{
  "name": "vpc_001",
  "type": 2,
  "member_type": "instance",
  "port": 15565,
  "balance_strategy": 1,
  "id": "c3e6a7d85d9e47be89dfcc3cd37405d7",
  "create_time": "2018-07-27T12:30:48Z",
  "status": 1,
  "vpc_health_config": {
    "protocol": "http",
    "path": "/hc",
    "port": 15563,
    "threshold_normal": 5,
    "threshold_abnormal": 5,
    "time_out": 30,
    "time_interval": 200,
    "http_code": "205",
    "id": "f26c1b158f2e40f2b531cf5c1b5e05e5",
    "vpc_id": "c3e6a7d85d9e47be89dfcc3cd37405d7",
    "create_time": "2018-07-27T12:30:48Z"
  },
  "vpc_instances": [
    {
      "instance_id": "instance01",
      "instance_name": "instance_name01",
      "host": "127.0.0.1",
      "weight": 10,
      "id": "c3bc73605a8b400793363c87574fbad7",
      "vpc_id": "c3e6a7d85d9e47be89dfcc3cd37405d7",
      "status": 1,
      "create_time": "2018-07-27T12:30:48Z"
    }
  ]
}
```

Status Codes

Table 5-507 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.18.6 Querying the VPC channel List

Function

This API is used to query the list of VPC channels that have been created.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-508 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/vpc-channels[?page_size, page_no, id, name, vpc_type]

o

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **id**, **name**, **vpc_type**, **page_size**, and **page_no**.

Table 5-509 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	VPC channel ID

Parameter	Mandatory	Type	Description
name	No	String	VPC channel name
vpc_type	No	Integer	VPC channel type, which can be:
page_size	No	Integer	Number of VPC channels displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .
precise_search	No	String	Parameter name (name) for exact matching

Request

N/A

Response

Table 5-510 Parameter description

Parameter	Type	Description
total	Integer	Total number of VPC channels that match the query conditions
size	Integer	Length of the returned VPC channel list
vpcs	Dictionary	VPC channel list

Table 5-511 VPC channel parameter description

Parameter	Type	Description
id	String	VPC channel ID
name	String	VPC channel name
type	Integer	VPC channel type, which can be: • 2: fast channel with the load balancing function

Parameter	Type	Description
member_type	String	Member type of the VPC channel, which can be: - ip (not supported currently) - instance
status	Integer	VPC channel status, which can be: 1: normal 2: abnormal
port	Integer	Host port of the VPC channel
balance_strategy	Integer	Distribution algorithm, which can be: 1: WRR 2: WLC 3: SH 4: URI hashing
create_time	Timestamp	Time when the VPC channel is created

Example response:

```
{
  "total": 2,
  "size": 2,
  "vpcs": [
    {
      "name": "Channel_1",
      "type": 1,
      "member_type": "instance",
      "port": 8080,
      "balance_strategy": 1,
      "id": "39c62689302a48fe9f4bd7cf5c052064",
      "create_time": "2018-04-24T12:07:58Z",
      "status": 1
    },
    {
      "name": "Channel_2",
      "type": 2,
      "member_type": "instance",
      "port": 8088,
      "balance_strategy": 1,
      "id": "e6831cbcbe2b45bbbc6318c2892f060b",
      "create_time": "2018-04-24T11:57:03Z",
      "status": 1
    }
  ]
}
```

Status Codes

Table 5-512 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.18.7 Adding Backend Instances (Cloud Servers)

Function

This API is used to add cloud servers to a specified VPC channel.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-513 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/vpc-channels/{id}/members

The following table lists the parameter in the URI.

Table 5-514 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	VPC channel ID

Request

Table 5-515 Parameter description

Parameter	Mandatory	Type	Description
vpc_instances	Yes	Dictionary	Backend instance list

Table 5-516 Backend instance details

Parameter	Mandatory	Type	Description
instance_name	Yes	String	Cloud server name The name must contain 1–64 characters. Only letters, digits, periods (.), hyphens (-), and underscores (_) are allowed.
instance_id	Yes	String	Cloud server ID The ID must contain 1–64 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
weight	Yes	Integer	Cloud server weight The larger the weight is, the more requests are forwarded to the cloud server. Range: 1–100

Example request:

```
{
  "vpc_instances": [
    {
      "instance_id": "instance02",
      "instance_name": "instance_name02",
      "weight": 10
    }
  ]
}
```

Response

Table 5-517 Parameter description

Parameter	Type	Description
total	Integer	Total number of cloud servers under the VPC channel

Parameter	Type	Description
size	Integer	Total number of cloud servers returned
vpc_instances	Dictionary	Cloud server list

Table 5-518 Backend instance details

Parameter	Type	Description
id	String	Backend instance object ID
vpc_id	String	VPC channel ID
status	Integer	Status of the backend instance object
instance_name	String	Cloud server name
instance_id	String	Cloud server ID
host	String	Cloud server IP address
weight	Integer	Cloud server weight The larger the weight is, the more requests are forwarded to the cloud server. Range: 1-100
create_time	Timestamp	Time when the cloud server is added to the VPC channel

Example response:

```
{
  "total": 2,
  "size": 2,
  "vpc_instances": [
    {
      "instance_id": "instance02",
      "instance_name": "instance_name02",
      "host": "127.0.0.2",
      "weight": 10,
      "id": "680e42fab429447ca23b9623107523d9",
      "vpc_id": "c3e6a7d85d9e47be89dfcc3cd37405d7",
      "status": 1,
      "create_time": "2018-07-27T12:42:32Z"
    },
    {
      "instance_id": "instance01",
      "instance_name": "instance_name01",
      "host": "127.0.0.1",
      "weight": 10,
      "id": "c3bc73605a8b400793363c87574fbad7",
      "vpc_id": "c3e6a7d85d9e47be89dfcc3cd37405d7",
      "status": 1,
      "create_time": "2018-07-27T12:30:48Z"
    }
  ]
}
```

```
}  
]  
}
```

Status Codes

Table 5-519 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.18.8 Deleting a Backend Instance (Cloud Server)

Function

This API is used to delete a cloud server of a specified VPC channel.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-520 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/vpc-channels/{id}/members/{inst_id}

The following table lists the parameters in the URI.

Table 5-521 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	VPC channel ID
inst_id	Yes	String	Backend instance object ID

Request

N/A

Response

N/A

Status Codes

Table 5-522 Status codes

Status Code	Description
204	No Content
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.18.9 Querying the Backend Instance List (Cloud Server List)

Function

This API is used to query the cloud servers of a specified VPC channel.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-523 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/vpc-channels/{id}/members[?page_size, page_no, name]

 NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **name**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-524 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	VPC channel ID
name	No	String	Cloud server name
page_size	No	Integer	Number of cloud servers displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .

Request

N/A

Response

Table 5-525 Parameter description

Parameter	Type	Description
total	Integer	Total number of cloud servers that match the query conditions
size	Integer	Length of the returned cloud server list
vpc_instances	Dictionary	Cloud server list

Table 5-526 Backend instance details

Parameter	Type	Description
id	String	Backend instance object ID
vpc_id	String	VPC channel ID
status	Integer	Status of the backend instance object
instance_name	String	Cloud server name
instance_id	String	Cloud server ID
host	String	Cloud server IP address

Parameter	Type	Description
weight	Integer	Cloud server weight The larger the weight is, the more requests are forwarded to the cloud server. Range: 1–100
create_time	Timestamp	Time when the cloud server is added to the VPC channel

Example response:

```
{
  "total": 2,
  "size": 2,
  "vpc_instances": [
    {
      "instance_id": "instance02",
      "instance_name": "instance_name02",
      "host": "127.0.0.2",
      "weight": 10,
      "id": "680e42fab429447ca23b9623107523d9",
      "vpc_id": "c3e6a7d85d9e47be89dfcc3cd37405d7",
      "status": 1,
      "create_time": "2018-07-27T12:42:32Z"
    },
    {
      "instance_id": "instance01",
      "instance_name": "instance_name01",
      "host": "127.0.0.1",
      "weight": 10,
      "id": "c3bc73605a8b400793363c87574fbad7",
      "vpc_id": "c3e6a7d85d9e47be89dfcc3cd37405d7",
      "status": 1,
      "create_time": "2018-07-27T12:30:48Z"
    }
  ]
}
```

Status Codes

Table 5-527 Status codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Server Internal Error

5.19 Querying Metrics

5.19.1 Querying API Calls Within a Period

Function

This API is used to query the number of times an API is called during a period. The query can be based on 1 minute, 1 hour, or 1 day.

- If the time range is within one hour, the server returns data of the latest N minutes, with the number of API calls collected every minute.
- If the time range is within one day, the server returns data of the latest N hours (or N + 1 hours if N is not an integer), with the number of API calls collected every hour. For example, if the time range is within 2 to 3 hours, data of the latest 2 + 1 hours will be returned.
- If the time range is longer than one day, the server returns data of the latest N days (or N + 1 days if N is not an integer), with the number of API calls collected every day.

NOTE

For security purposes, clear your operation records, including but not limited to records in the `~/.bash_history` and `/var/log/messages` directories (if any), after running the `curl` command on the server to query information.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-528 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/statistics/api/latest?api_id=[api_id]&duration=[duration]

Request

Table 5-529 Parameter description of statistic data

Parameter	Mandatory	Type	Description
api_id	Yes	String	API ID

Parameter	Mandatory	Type	Description
duration	Yes	String	Time range (unit: h or m). For example, 1h refers to the latest 1 hour and 1m refers to the latest 1 minute.

Response

Table 5-530 Parameter description

Parameter	Type	Description	Operation Type
code	String	Response code	R
msg	String	Response message	R
start_time	Long	Timestamp (UTC) of the start time	R
end_time	Long	Timestamp (UTC) of the end time	R
list	Structure	Statistic data	R

Table 5-531 Parameter description of statistic data

Parameter	Type	Description	Operation Type
cycle	String	Interval (reserved)	R
api_id	String	API ID	R
current_minute	Long	Timestamp (UTC) of API access	R
group_id	String	API group ID	R
provider	String	API provider	R
req_count	Integer	Total number of requests	R
max_latency	Integer	Maximum latency	R
avg_latency	Double	Average latency	R
max_backend_latency	Integer	Maximum backend latency	R

Parameter	Type	Description	Operation Type
avg_backend_latency	Double	Average backend latency	R
max_inner_latency	Integer	Maximum gateway latency	R
avg_inner_latency	Double	Average gateway latency	R
output_throughput	Integer	Downstream throughput (bytes)	R
input_throughput	Integer	Upstream throughput (bytes)	R
req_count4xx	Integer	Total number of 4xx response codes	R
req_count5xx	Integer	Total number of 5xx response codes	R
req_count2xx	Integer	Total number of 2xx response codes	R
req_count_error	Integer	Number of errors	R
register_time	String	Recording time (yyy-MM-dd HH:mm:ss)	R
req_time	String	API request time (yyy-MM-dd HH:mm:ss)	R
status	Integer	Status (reserved)	R

Example response:

```
{
  "code": "APIG.0000",
  "msg": "",
  "start_time": 1524735000,
  "end_time": 1524735000,
  "list": [
    {
      "api_id": "ae12b59fef2e4c6b8e01d44e98b738c0",
      "current_minute": 1524735000,
      "group_id": "26463e4b2445415eabb55b2414012989",
      "provider": "d4ef919b31bd43d3927c5d46c71b68c4",
      "req_count": 45,
      "max_latency": 59,
      "avg_latency": 2.53,
      "max_backend_latency": 0,
      "avg_backend_latency": 0,
      "max_inner_latency": 59,
      "avg_inner_latency": 2.53,
      "output_throughput": 31815,
      "input_throughput": 334474,
    }
  ]
}
```

```
"req_count4xx":0,
"req_count5xx":0,
"req_count2xx":45,
"req_count_error":0,
"register_time":"2018-04-26 17:30:48",
"req_time":"2018-04-26 17:30:00",
"status":1
}
]
```

Status Codes

Table 5-532 Status codes

Status Code	Description
200	Query Success

5.19.2 Querying API Calls Under an API Group in the Last One Hour

Function

This API is used to query the number of times APIs are called within a period by API group ID. The query is based on 1 minute. If the time range is within one hour, the server returns the number of API calls made every minute.

NOTE

For security purposes, clear your operation records, including but not limited to records in the `~/.bash_history` and `/var/log/messages` directories (if any), after running the `curl` command on the server to query information.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-533 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/statistics/group/latest?group_id=[group_id]

Request

Table 5-534 Parameter description

Parameter	Mandatory	Type	Description
group_id	Yes	String	API group ID

Response

Table 5-535 Parameter description

Parameter	Type	Description	Operation Type
code	String	Response code	R
msg	String	Response message	R
start_time	Long	Timestamp (UTC) of the start time	R
end_time	Long	Timestamp (UTC) of the end time	R
list	Structure	Statistic data	R

Table 5-536 Parameter description of statistic data

Parameter	Type	Description	Operation Type
group_id	String	API group ID	R
current_minute	Long	Timestamp (UTC)	R
provider	String	API provider	R
req_count	Integer	Total number of requests	R
max_latency	Integer	Maximum latency (ms)	R
avg_latency	Double	Average latency (ms)	R
output_throughput	Integer	Downstream throughput (bytes)	R

Parameter	Type	Description	Operation Type
input_throughput	Integer	Upstream throughput (bytes)	R
req_count4xx	Integer	Total number of 4xx response codes	R
req_count5xx	Integer	Total number of 5xx response codes	R
req_count2xx	Integer	Total number of 2xx response codes	R
req_count_error	Integer	Number of errors	R
register_time	String	Recording time (yyyy-MM-dd HH:mm:ss)	R
req_time	String	Request time (yyyy-MM-dd HH:mm:ss)	R

Example response:

```
{
  "code": "000000",
  "msg": "",
  "list": [{
    "group_id": "d7b52683-341b-4234-8261-66b4cfbfbda5",
    "current_minute": 1516849440,
    "provider": "205fa874817a4dcfae9222a3be4725e8",
    "req_count": 1981,
    "max_latency": 199,
    "avg_latency": 98.17,
    "output_throughput": 694483,
    "input_throughput": 694483,
    "req_count4xx": 669,
    "req_count5xx": 312,
    "req_count2xx": 327,
    "req_count_error": 981,
    "register_time": "2018-01-25 11:04:09",
    "req_time": "2018-01-25 11:04:00"
  }],
  "start_time": 1516845900,
  "end_time": 1516849440
}
```

Status Codes

Table 5-537 Status codes

Status Code	Description
200	Query Success

5.20 OpenAPI

5.20.1 Exporting All APIs in an API Group

Function

This API is used to export definitions of APIs in a specified API group.

The basic, full, or extended Swagger definitions of APIs belonging to the API group and published in a specified environment will be imported.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-538 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/openapi? env_id={0}&group_id={1}&define={2}&version={3}&type={4}

Request

Table 5-539 Parameter description

Parameter	Mandator y	Type	Description
env_id/env	Yes	String	ID of the environment where APIs in a specified group have been published. Both env_id (recommended) and env can indicate an environment ID. If the two parameters are available, the value of env_id takes the precedence.
group_id/ group	Yes	String	API group ID. Both group_id (recommended) and group can indicate a group ID. If the two parameters are available, the value of group_id takes the precedence.

Parameter	Mandatory	Type	Description
define	No	String	Definition scope of the APIs to be exported: • base: basic definition • full: full definition • all: extended definition The default value is base .
version	No	String	Version of the APIs after exporting. The default value is the current date and time.
type	No	String	Format for exporting API definitions. The value can be json or yaml . The default value is json .

Response

Table 5-540 Parameter description

Parameter	Mandatory	Type	Description
swagger	Yes	String	The value is fixed at 2.0 .
info	Yes	Object	See Table 5-541 .
host	Yes	String	Subdomain name bound to the API group
paths	Yes	Object	See parameter description of paths .
responses	Yes	Object	Common response, which can be referenced in {method} . For details, see Table 5-546 .
securityDefinitions	Yes	Object	Security authentication mode definition. For details, see Table 5-550 .
x-apigateway-access-controls	No	Object	Access control information. For details, see parameter description of x-apigateway-access-controls .
x-apigateway-ratelimits	No	Object	Request throttling information. For details, see parameter description of x-apigateway-ratelimits .

Table 5-541 Parameter description of info

Parameter	Mandatory	Type	Description
title	Yes	String	API group name
version	Yes	String	Version number. You can specify a version number or use the current date and time by default.
description	No	String	Description of the API group

Table 5-542 Parameter description of paths

Parameter	Mandatory	Type	Description
uri	Yes	Object	API access address. For details, see Table 5-543 .

Table 5-543 Parameter description of uri

Parameter	Mandatory	Type	Description
method	Yes	Object	API access method. For details, see Table 5-544 .

Table 5-544 Parameter description of method

Parameter	Mandatory	Type	Description
operationId	Yes	String	API name
description	No	String	API description
schemes	Yes	Object	API request protocol. HTTP and HTTPS are supported.
tags	No	Object	API tags
parameters	No	Object	Request parameter definitions. For details, see frontend parameter description .
responses	Yes	Object	Response definition. For details, see Table 5-546 .
security	No	Object	Security authentication mode. For details, see parameter description of security .

Parameter	Mandatory	Type	Description
x-apigateway-access-control	No	Object	Access control policy bound to the API
x-apigateway-backend	No	Object	Backend information. For details, see parameter description of x-apigateway-backend .
x-apigateway-backend-policies	No	Object	Backend policy information. For details, see parameter description of x-apigateway-backend-policies .
x-apigateway-cors	No	Boolean	Indicates whether CORS is supported.
x-apigateway-match-mode	No	String	Route matching mode
x-apigateway-ratelimit	No	String	Name of the request throttling policy bound to the API
x-apigateway-request-type	No	String	API type

Table 5-545 Frontend parameter description

Parameter	Mandatory	Type	Description
maximum	No	Float	Maximum value of a number type parameter
minimum	No	Float	Minimum value of a number type parameter
maxLength	No	Integer	Maximum length of a string type parameter
minLength	No	Integer	Minimum length of a string type parameter
pattern	No	String	Regular expression of the parameter value
type	No	String	Parameter type
default	No	String	Default value
description	No	String	Parameter description
name	No	String	Parameter name
in	No	String	Parameter location, which can be path , header , query , formData , or body

Parameter	Mandatory	Type	Description
required	No	Boolean	Indicates whether the parameter is required. The parameter is required when its location is path .

Table 5-546 Parameter description of responses

Parameter	Mandatory	Type	Description
default	No	Object	Default response, which will be used when no status codes are defined
status_code	No	Object	Response status code. For details, see Table 5-548 .
x-apigateway-result-failure-sample	No	String	Example response for a failed request
x-apigateway-result-normal-sample	No	String	Example response for a successful request

Table 5-547 Parameter description of security

Parameter	Mandatory	Type	Description
apig-auth-type	No	Object	Security authentication mode. This parameter is a null array. Options: • apig-auth-app: App authentication • apig-auth-iam: IAM authentication • Null: No authentication required

Table 5-548 Parameter description of status_code

Parameter	Mandatory	Type	Description
description	No	String	Response description
schema	No	Object	Response body. For details, see Table 5-549 .

Table 5-549 Parameter description of schema

Parameter	Mandatory	Type	Description
description	No	String	Response body
type	No	String	Body type, which can be FORM or STREAM

Table 5-550 Parameter description of securityDefinitions

Parameter	Mandatory	Type	Description
name	Yes	Object	Security authentication mode. For details, see Table 5-551 .

Table 5-551 Parameter description of name

Parameter	Mandatory	Type	Description
type	Yes	String	Authentication type. apiKey is supported.
name	Yes	String	Name of apiKey
in	Yes	String	Location of apiKey
x-apigateway-auth-type	Yes	String	Authentication type extended based on apiKey. Authentication types AppSigv1, IAM, and IAM_NONE are supported.

Table 5-552 Parameter description of x-apigateway-backend

Parameter	Mandatory	Type	Description
type	Yes	String	Backend type. The options include HTTP , HTTP-VPC , FUNCTION , and MOCK .
parameters	No	Object	Backend parameters. For details, see backend parameter description .

Parameter	Mandatory	Type	Description
backend_definition	Yes	Object	Backend definition The following backend definitions are supported: • httpEndpoints: See parameter description of backend httpEndpoints. • httpVpcEndpoints: See parameter description of backend httpVpcEndpoints. • functionEndpoints: See parameter description of backend functionEndpoints. • mockEndpoints: See parameter description of backend mockEndpoints.

Table 5-553 Parameter description of x-apigateway-backend-policies

Parameter	Mandatory	Type	Description
type	Yes	String	Backend type. The options include HTTP , HTTP-VPC , FUNCTION , and MOCK .
name	Yes	String	Backend policy name
parameters	No	Object	Backend parameters. For details, see backend parameter description .
backend_definition	Yes	Object	Backend definition The following backend definitions are supported: • httpEndpoints: See parameter description of backend httpEndpoints. • httpVpcEndpoints: See parameter description of backend httpVpcEndpoints. • functionEndpoints: See parameter description of backend functionEndpoints. • mockEndpoints: See parameter description of backend mockEndpoints.

Parameter	Mandatory	Type	Description
conditions	Yes	Object	Policy conditions. For details, see parameter description of conditions .
effectMode	Yes	String	Effective mode of the backend policy. The options include ANY and ALL .

Table 5-554 Backend parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name, which consists of a maximum of 32 bytes, starting with a letter. Only letters, digits, periods (.), hyphens (-), and underscores (_) are allowed. The names of header parameters are not case-sensitive.
value	Yes	String	Parameter value, which is a parameter name if the parameter comes from a request
in	Yes	String	Parameter location, which can be header , query , or path
origin	Yes	String	Parameter mapping source. The options include REQUEST and CONSTANT .
description	No	String	Parameter meaning

Table 5-555 Parameter description of backend httpEndpoints

Parameter	Mandatory	Type	Description
address	Yes	String	Backend service address. The format is <i><Domain name or IP address>.[Port number]</i>
scheme	Yes	String	Backend request protocol. HTTP and HTTPS are supported.
method	Yes	String	Backend request method. The options include GET , POST , PUT , DELETE , HEAD , OPTIONS , PATCH , and ANY .

Parameter	Mandatory	Type	Description
path	Yes	String	Backend request path, which can contain variables.
timeout	No	Integer	Backend request timeout in milliseconds. The value ranges from 1 to 60,000, and the default value is 5000 .
description	No	String	Backend description

Table 5-556 Parameter description of backend httpVpcEndpoints

Parameter	Mandatory	Type	Description
name	Yes	Array	VPC channel name
scheme	Yes	String	Backend request protocol. HTTP and HTTPS are supported.
method	Yes	String	Backend request method. The options include GET, POST, PUT, DELETE, HEAD, OPTIONS, PATCH , and ANY .
path	Yes	String	Backend request path, which can contain variables.
timeout	No	Integer	Backend request timeout in milliseconds. The value ranges from 1 to 60,000, and the default value is 5000 .
host	No	String	VPC channel proxy host
description	No	String	Backend description

Table 5-557 Parameter description of backend functionEndpoints

Parameter	Mandatory	Type	Description
function-urn	Yes	String	Function URN
version	Yes	String	Function version
invocation-type	Yes	String	Function invocation type. The value can be async or sync .
timeout	No	Integer	Function timeout in milliseconds. The value ranges from 1 to 60,000, and the default value is 5000 .

Parameter	Mandatory	Type	Description
description	No	String	Backend description

Table 5-558 Parameter description of backend mockEndpoints

Parameter	Mandatory	Type	Description
result-content	Yes	String	Mock response
description	No	String	Backend description

Table 5-559 Parameter description of conditions

Parameter	Mandatory	Type	Description
type	Yes	String	Policy condition type. The options include equal , enum , and pattern .
value	Yes	String	Policy condition value
origin	Yes	String	Policy condition source. The options include source and request .
parameter	No	String	Input parameter name if the origin parameter is set to request .

Table 5-560 Parameter description of x-apigateway-access-controls

Parameter	Mandatory	Type	Description
acl_name	No	Object	Access control policy. For details, see parameter description of acl_name .

Table 5-561 Parameter description of acl_name

Parameter	Mandatory	Type	Description
acl-type	Yes	String	Access control effect. The options include PERMIT and DENY .
entity-type	Yes	String	Access control object. Only IP addresses and accounts are supported.

Parameter	Mandatory	Type	Description
value	Yes	String	Access control values, which are separated with commas (,).

Table 5-562 Parameter description of x-apigateway-ratelimits

Parameter	Mandatory	Type	Description
throttle_name	No	Object	Request throttling policy. For details, see parameter description of throttle_name .

Table 5-563 Parameter description of throttle_name

Parameter	Mandatory	Type	Description
api-limit	Yes	Integer	Maximum number of times an API can be called
user-limit	No	Integer	Number of times the API can be called by a user
app-limit	No	Integer	Number of times the API can be called by an app
ip-limit	No	Integer	Number of times the API can be called by an IP address
interval	Yes	Integer	Throttling period
unit	Yes	String	Throttling unit, which can be SECOND , MINUTE , HOURL , or DAY
shared	No	Boolean	Whether to share the throttling limits among APIs
special	No	Object	Excluded request throttling configurations. For details, see parameter description of special .

Table 5-564 Parameter description of special

Parameter	Mandatory	Type	Description
type	Yes	String	Excluded request throttling type, which can be APP or USER

Parameter	Mandatory	Type	Description
limit	Yes	Integer	Access limit
instance	Yes	String	Excluded app or user

Example response:

```
{
  "swagger": "2.0",
  "info": {
    "description": "api group test",
    "title": "APIGroup_test",
    "version": "2019-09-12-17:38:10"
  },
  "host": "6b075335476a4943bf70c3db1343c912.apigw.example.com",
  "paths": {
    "/test/{path}": {
      "get": {
        "security": [
          {
            "apig-auth-app": []
          }
        ],
        "description": "api test",
        "schemes": [
          "https"
        ],
        "operationId": "API_test",
        "parameters": [
          {
            "type": "string",
            "description": "header parameter",
            "name": "header",
            "in": "header",
            "required": true
          },
          {
            "type": "string",
            "description": "path parameter",
            "name": "path",
            "in": "path",
            "required": true
          },
          {
            "type": "number",
            "default": "123",
            "description": "query parameter",
            "name": "query",
            "in": "query"
          }
        ],
        "responses": {
          "default": {
            "$ref": "#/responses/default"
          },
          "x-apigateway-result-failure-sample": "",
          "x-apigateway-result-normal-sample": "success"
        },
        "x-apigateway-backend": {
          "httpEndpoints": {
            "address": "1.1.1.1:443",
            "description": "",
            "method": "GET",
```

```
    "path": "/test/{path}",
    "scheme": "https",
    "timeout": 5000
  },
  "parameters": [
    {
      "description": "",
      "in": "HEADER",
      "name": "header",
      "origin": "REQUEST",
      "value": "header"
    },
    {
      "description": "",
      "in": "PATH",
      "name": "path",
      "origin": "REQUEST",
      "value": "path"
    },
    {
      "description": "",
      "in": "QUERY",
      "name": "query",
      "origin": "REQUEST",
      "value": "query"
    }
  ],
  "type": "HTTP"
},
"x-apigateway-backend-policies": [
  {
    "conditions": [
      {
        "origin": "param",
        "parameter": "path",
        "type": "exact",
        "value": "path"
      },
      {
        "origin": "source",
        "parameter": "",
        "type": "",
        "value": "1.0.0.0/8"
      }
    ],
    "effectMode": "ANY",
    "httpVpcEndpoints": {
      "method": "POST",
      "name": "VPC_n9ct",
      "path": "/",
      "scheme": "HTTPS",
      "timeout": 5000
    },
    "name": "policy_test",
    "type": "HTTP-VPC"
  }
],
"x-apigateway-cors": false,
"x-apigateway-match-mode": "NORMAL",
"x-apigateway-request-type": "public"
}
},
"responses": {
  "default": {
    "description": "response example"
  }
},
"securityDefinitions": {
```

```
"apig-auth-app": {
  "type": "apiKey",
  "name": "Authorization",
  "in": "header",
  "x-apigateway-auth-type": "AppSigv1"
},
"apig-auth-iam": {
  "type": "apiKey",
  "name": "unused",
  "in": "header",
  "x-apigateway-auth-type": "IAM"
}
}
```

Status Codes

Table 5-565 Status codes

Status Code	Description
200	OK
400	bad request
401	unauthorized
403	forbidden
500	server internal error

5.20.2 Exporting Multiple APIs

Function

This API is used to export the basic, full, or extended Swagger definition of specified APIs by their IDs.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-566

Request Method	URI
POST	/v1.0/apigw/openapi/apis? env_id={0}&define={2}&version={3}&type={4}

The following table lists the parameter in the URI.

Table 5-567 Parameter description

Parameter	Mandatory	Type	Description
env_id/env	Yes	String	ID of the environment where APIs in a specified group have been published. Both env_id (recommended) and env can indicate an environment ID. If the two parameters are available, the value of env_id takes the precedence.
define	No	String	Definition scope of the APIs to be exported: • base: basic definition • full: full definition • all: extended definition The default value is base .
version	No	String	Version of the APIs after exporting. The default value is the current date and time.
type	No	String	Format for exporting API definitions. The value can be json or yaml . The default value is json .

Request

Table 5-568 Parameter description

Location	Mandatory	Type	Description
body	Yes	String Array	IDs of the APIs to be exported

Example request:

```
["81efcfd94b8747a0b21e8c04144a4e8c","7addcd00cfab433984b1d8bf2fe08aaa"]
```

Response

Table 5-569 Parameter description

Parameter	Mandatory	Type	Description
swagger	Yes	String	The value is fixed at 2.0 .
info	Yes	Object	For details, see Table 5-570 .
host	Yes	String	Subdomain name bound to the API group
paths	Yes	Object	See parameter description of paths .
responses	Yes	Object	Common response, which can be referenced in {method} . For details, see Table 5-575 .
securityDefinitions	Yes	Object	Security authentication mode definition. For details, see Table 5-579 .
x-apigateway-access-controls	No	Object	Access control information. For details, see parameter description of x-apigateway-access-controls .
x-apigateway-ratelimits	No	Object	Request throttling information. For details, see parameter description of x-apigateway-ratelimits .

Table 5-570 Parameter description of info

Parameter	Mandatory	Type	Description
title	Yes	String	API group name
version	Yes	String	Version number. You can specify a version number or use the current date and time by default.
description	No	String	Description of the API group

Table 5-571 Parameter description of paths

Parameter	Mandatory	Type	Description
uri	Yes	Object	API access address. For details, see Table 5-572 .

Table 5-572 Parameter description of uri

Parameter	Mandatory	Type	Description
method	Yes	Object	API access method. For details, see Table 5-573 .

Table 5-573 Parameter description of method

Parameter	Mandatory	Type	Description
operationId	Yes	String	API name
description	No	String	API description
schemes	Yes	Object	API request protocol. HTTP and HTTPS are supported.
tags	No	Object	API tags
parameters	No	Object	Request parameter definitions. For details, see frontend parameter description .
responses	Yes	Object	Response definition. For details, see Table 5-575 .
security	No	Object	Security authentication mode. For details, see parameter description of security .
x-apigateway-access-control	No	Object	Access control policy bound to the API
x-apigateway-backend	No	Object	Backend information. For details, see parameter description of x-apigateway-backend .
x-apigateway-backend-policies	No	Object	Backend policy information. For details, see parameter description of x-apigateway-backend-policies .
x-apigateway-cors	No	Boolean	Indicates whether CORS is supported.
x-apigateway-match-mode	No	String	Route matching mode
x-apigateway-ratelimit	No	String	Name of the request throttling policy bound to the API
x-apigateway-request-type	No	String	API type

Table 5-574 Frontend parameter description

Parameter	Mandatory	Type	Description
maximum	No	Float	Maximum value of a number type parameter
minimum	No	Float	Minimum value of a number type parameter
maxLength	No	Integer	Maximum length of a string type parameter
minLength	No	Integer	Minimum length of a string type parameter
pattern	No	String	Regular expression of the parameter value
type	No	String	Type
default	No	String	Default value
description	No	String	Parameter description
name	No	String	Parameter name
in	No	String	Parameter location, which can be path , header , query , formData , or body
required	No	Boolean	Whether the parameter is required. The parameter is required when its location is path .

Table 5-575 Parameter description of responses

Parameter	Mandatory	Type	Description
default	No	Object	Default response, which will be used when no status codes are defined
status_code	No	Object	Response status code. For details, see Table 5-577 .
x-apigateway-result-failure-sample	No	String	Example response for a failed request
x-apigateway-result-normal-sample	No	String	Example response for a successful request

Table 5-576 Parameter description of security

Parameter	Mandatory	Type	Description
apig-auth-type	No	Object	Security authentication mode. This parameter is a null array. Options: • apig-auth-app: App authentication • apig-auth-iam: IAM authentication • Null: No authentication required

Table 5-577 Parameter description of status code

Parameter	Mandatory	Type	Description
description	No	String	Response description
schema	No	Object	Response body. For details, see Table 5-578 .

Table 5-578 Parameter description of schema

Parameter	Mandatory	Type	Description
description	No	String	Body description
type	No	String	Body type, which can be FORM or STREAM

Table 5-579 Parameter description of securityDefinitions

Parameter	Mandatory	Type	Description
name	Yes	Object	Security authentication mode. For details, see Table 5-580 .

Table 5-580 Parameter description of name

Parameter	Mandatory	Type	Description
type	Yes	String	Authentication type. apiKey is supported.

Parameter	Mandatory	Type	Description
name	Yes	String	Name of apiKey
in	Yes	String	Location of apiKey
x-apigateway-auth-type	Yes	String	Authentication type extended based on apiKey. Authentication types AppSigv1, IAM, and IAM_NONE are supported.

Table 5-581 Parameter description of x-apigateway-backend

Parameter	Mandatory	Type	Description
type	Yes	String	Backend type. The options include HTTP , HTTP-VPC , FUNCTION , and MOCK .
parameters	No	Object	Backend parameters. For details, see backend parameter description .
backend_definition	Yes	Object	Backend definition The following backend definitions are supported: • httpEndpoints: See parameter description of backend httpEndpoints. • httpVpcEndpoints: See parameter description of backend httpVpcEndpoints. • functionEndpoints: See parameter description of backend functionEndpoints. • mockEndpoints: See parameter description of backend mockEndpoints.

Table 5-582 Parameter description of x-apigateway-backend-policies

Parameter	Mandatory	Type	Description
type	Yes	String	Backend type. The options include HTTP , HTTP-VPC , FUNCTION , and MOCK .
name	Yes	String	Backend policy name

Parameter	Mandatory	Type	Description
parameters	No	Object	Backend parameters. For details, see backend parameter description .
backend_definition	Yes	Object	Backend definition The following backend definitions are supported: • httpEndpoints: See parameter description of backend httpEndpoints. • httpVpcEndpoints: See parameter description of backend httpVpcEndpoints. • functionEndpoints: See parameter description of backend functionEndpoints. • mockEndpoints: See parameter description of backend mockEndpoints.
conditions	Yes	Object	Policy conditions. For details, see parameter description of conditions .
effectMode	Yes	String	Effective mode of the backend policy. The options include ANY and ALL .

Table 5-583 Backend parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name, which consists of a maximum of 32 bytes, starting with a letter. Only letters, digits, periods (.), hyphens (-), and underscores (_) are allowed. The names of header parameters are not case-sensitive.
value	Yes	String	Parameter value, which is a parameter name if the parameter comes from a request
in	Yes	String	Parameter location, which can be header , query , or path
origin	Yes	String	Parameter mapping source. The options include REQUEST and CONSTANT .

Parameter	Mandatory	Type	Description
description	No	String	Parameter meaning

Table 5-584 Parameter description of backend httpEndpoints

Parameter	Mandatory	Type	Description
address	Yes	String	Backend service address. The format is <i><Domain name or IP address>:[Port number]</i>
scheme	Yes	String	Backend request protocol. HTTP and HTTPS are supported.
method	Yes	String	Backend request method. The options include GET , POST , PUT , DELETE , HEAD , OPTIONS , PATCH , and ANY .
path	Yes	String	Backend request path, which can contain variables.
timeout	No	Integer	Backend request timeout in milliseconds. The value ranges from 1 to 60,000, and the default value is 5000 .
description	No	String	Backend description

Table 5-585 Parameter description of backend httpVpcEndpoints

Parameter	Mandatory	Type	Description
name	Yes	Array	VPC channel name
scheme	Yes	String	Backend request protocol. HTTP and HTTPS are supported.
method	Yes	String	Backend request method. The options include GET , POST , PUT , DELETE , HEAD , OPTIONS , PATCH , and ANY .
path	Yes	String	Backend request path, which can contain variables.
timeout	No	Integer	Backend request timeout in milliseconds. The value ranges from 1 to 60,000, and the default value is 5000 .
host	No	String	VPC channel proxy host

Parameter	Mandatory	Type	Description
description	No	String	Backend description

Table 5-586 Parameter description of backend functionEndpoints

Parameter	Mandatory	Type	Description
function-urn	Yes	String	Function URN
version	Yes	String	Function version
invocation-type	Yes	String	Function invocation type. The value can be async or sync .
timeout	No	Integer	Function timeout in milliseconds. The value ranges from 1 to 60,000, and the default value is 5000 .
description	No	String	Backend description

Table 5-587 Parameter description of backend mockEndpoints

Parameter	Mandatory	Type	Description
result-content	Yes	String	Mock response
description	No	String	Backend description

Table 5-588 Parameter description of conditions

Parameter	Mandatory	Type	Description
type	Yes	String	Policy condition type. The options include equal , enum , and pattern .
value	Yes	String	Policy condition value
origin	Yes	String	Policy condition source. The options include source and request .
parameter	No	String	Input parameter name if the origin parameter is set to request .

Table 5-589 Parameter description of x-apigateway-access-controls

Parameter	Mandatory	Type	Description
acl_name	No	Object	Access control policy. For details, see parameter description of acl_name .

Table 5-590 Parameter description of acl_name

Parameter	Mandatory	Type	Description
acl-type	Yes	String	Access control effect. The options include PERMIT and DENY .
entity-type	Yes	String	Access control object. Only IP addresses and accounts are supported.
value	Yes	String	Access control values, which are separated with commas (,).

Table 5-591 Parameter description of x-apigateway-ratelimits

Parameter	Mandatory	Type	Description
throttle_name	No	Object	Request throttling policy. For details, see parameter description of throttle_name .

Table 5-592 Parameter description of throttle_name

Parameter	Mandatory	Type	Description
api-limit	Yes	Integer	Maximum number of times an API can be called
user-limit	No	Integer	Number of times the API can be called by a user
app-limit	No	Integer	Number of times the API can be called by an app
ip-limit	No	Integer	Number of times the API can be called by an IP address
interval	Yes	Integer	Throttling period

Parameter	Mandatory	Type	Description
unit	Yes	String	Throttling unit, which can be SECOND , MINUTE , HOURL , or DAY
shared	No	Boolean	Whether to share the throttling limits among APIs
special	No	Object	Excluded request throttling configurations. For details, see parameter description of special .

Table 5-593 Parameter description of special

Parameter	Mandatory	Type	Description
type	Yes	String	Excluded request throttling type, which can be APP or USER
limit	Yes	Integer	Access limit
instance	Yes	String	Excluded app or user

Example response:

```
{
  "swagger": "2.0",
  "info": {
    "description": "api group test",
    "title": "APIGroup_test",
    "version": "2019-09-12-17:38:10"
  },
  "host": "6b075335476a4943bf70c3db1343c912.apigw.example.com",
  "paths": {
    "/test/{path}": {
      "get": {
        "security": [
          {
            "apig-auth-app": []
          }
        ],
        "description": "api test",
        "schemes": [
          "https"
        ],
        "operationId": "API_test",
        "parameters": [
          {
            "type": "string",
            "description": "header parameter",
            "name": "header",
            "in": "header",
            "required": true
          },
          {
            "type": "string",
            "description": "path parameter",
```

```
        "name": "path",
        "in": "path",
        "required": true
      },
      {
        "type": "number",
        "default": "123",
        "description": "query parameter",
        "name": "query",
        "in": "query"
      }
    ],
    "responses": {
      "default": {
        "$ref": "#/responses/default"
      },
      "x-apigateway-result-failure-sample": "",
      "x-apigateway-result-normal-sample": "success"
    },
    "x-apigateway-backend": {
      "httpEndpoints": {
        "address": "1.1.1.1:443",
        "description": "",
        "method": "GET",
        "path": "/test/{path}",
        "scheme": "https",
        "timeout": 5000
      },
      "parameters": [
        {
          "description": "",
          "in": "HEADER",
          "name": "header",
          "origin": "REQUEST",
          "value": "header"
        },
        {
          "description": "",
          "in": "PATH",
          "name": "path",
          "origin": "REQUEST",
          "value": "path"
        },
        {
          "description": "",
          "in": "QUERY",
          "name": "query",
          "origin": "REQUEST",
          "value": "query"
        }
      ],
      "type": "HTTP"
    },
    "x-apigateway-backend-policies": [
      {
        "conditions": [
          {
            "origin": "param",
            "parameter": "path",
            "type": "exact",
            "value": "path"
          },
          {
            "origin": "source",
            "parameter": "",
            "type": "",
            "value": "1.0.0.0/8"
          }
        ]
      }
    ]
  },
}
```



```
        "effectMode": "ANY",
        "httpVpcEndpoints": {
            "method": "POST",
            "name": "VPC_n9ct",
            "path": "/",
            "scheme": "HTTPS",
            "timeout": 5000
        },
        "name": "policy_test",
        "type": "HTTP-VPC"
    },
    ],
    "x-apigateway-cors": false,
    "x-apigateway-match-mode": "NORMAL",
    "x-apigateway-request-type": "public"
}
}
},
"responses": {
    "default": {
        "description": "response example"
    }
},
"securityDefinitions": {
    "apig-auth-app": {
        "type": "apiKey",
        "name": "Authorization",
        "in": "header",
        "x-apigateway-auth-type": "AppSigv1"
    },
    "apig-auth-iam": {
        "type": "apiKey",
        "name": "unused",
        "in": "header",
        "x-apigateway-auth-type": "IAM"
    }
}
}
```

Status Codes

Table 5-594 Status codes

Status Code	Description
200	OK
400	bad request
401	unauthorized
403	forbidden
500	server internal error

5.20.3 Importing APIs to a New API Group

Function

This API is used to import Swagger APIs to a new API group. Swagger files in JSON or YAML format are supported.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-595

Request Method	URI
POST	/v1.0/apigw/openapi

The following table lists the parameter in the URI.

Table 5-596 Parameter description

Parameter	Location	Mandatory	Type	Description
extend_mode	query	No	String	Extended definition import mode. The options include merge and override . If the extended definition conflicts with existing API definition, you can choose to retain or override the existing definition.

Request

Table 5-597 Parameter description

Parameter	Mandatory	Type	Description
swagger	Yes	String	The value is fixed at 2.0 .
info	Yes	Object	See Table 5-598 .
paths	Yes	Object	See parameter description of paths .
responses	No	Object	Common response, which can be referenced in {method} . For details, see Table 5-603 .
securityDefinitions	Yes	Object	Security authentication mode definition. For details, see Table 5-607 .
x-apigateway-access-controls	No	Object	Access control information. For details, see parameter description of x-apigateway-access-controls .

Parameter	Mandatory	Type	Description
x-apigateway-ratelimits	No	Object	Request throttling information. For details, see parameter description of x-apigateway-ratelimits .

Table 5-598 Parameter description of info

Parameter	Mandatory	Type	Description
title	Yes	String	API group name
version	No	String	Version number. You can specify a version number or use the current date and time by default.
description	No	String	Description of the API group

Table 5-599 Parameter description of paths

Parameter	Mandatory	Type	Description
uri	Yes	Object	API access address. For details, see Table 5-600 .

Table 5-600 Parameter description of uri

Parameter	Mandatory	Type	Description
method	Yes	Object	API access method. For details, see Table 5-601 .

Table 5-601 Parameter description of method

Parameter	Mandatory	Type	Description
operationId	No	String	API name
description	No	String	API description
schemes	No	Object	API request protocol. HTTP and HTTPS are supported.

Parameter	Mandatory	Type	Description
tags	No	Object	API tags
parameters	No	Object	Request parameter definitions. For details, see frontend parameter description .
responses	No	Object	Response definition. For details, see Table 5-603 .
security	No	Object	Security authentication mode. For details, see parameter description of security .
x-apigateway-access-control	No	Object	Access control policy bound to the API
x-apigateway-backend	No	Object	Backend information. For details, see parameter description of x-apigateway-backend .
x-apigateway-backend-policies	No	Object	Backend policy information. For details, see parameter description of x-apigateway-backend-policies .
x-apigateway-cors	No	Boolean	Indicates whether CORS is supported.
x-apigateway-match-mode	No	String	Route matching mode
x-apigateway-ratelimit	No	String	Name of the request throttling policy bound to the API
x-apigateway-request-type	No	String	API type

Table 5-602 Frontend parameter description

Parameter	Mandatory	Type	Description
maximum	No	Float	Maximum value of a number type parameter
minimum	No	Float	Minimum value of a number type parameter
maxLength	No	Integer	Maximum length of a string type parameter
minLength	No	Integer	Minimum length of a string type parameter
pattern	No	String	Regular expression of the parameter value

Parameter	Mandatory	Type	Description
type	No	String	Type
default	No	String	Default value
description	No	String	Parameter description
name	No	String	Parameter name
in	No	String	Parameter location, which can be path , header , query , formData , or body
required	No	Boolean	Whether the parameter is required. The parameter is required when its location is path .

Table 5-603 Parameter description of responses

Parameter	Mandatory	Type	Description
default	No	Object	Default response, which will be used when no status codes are defined
status_code	No	Object	Response status code. For details, see Table 5-605 .
x-apigateway-result-failure-sample	No	String	Example response for a failed request
x-apigateway-result-normal-sample	No	String	Example response for a successful request

Table 5-604 Parameter description of security

Parameter	Mandatory	Type	Description
apig-auth-type	No	Object	Security authentication mode. This parameter is a null array. Options: • apig-auth-app: App authentication • apig-auth-iam: IAM authentication • Null: No authentication required

Table 5-605 Parameter description of status_code

Parameter	Mandatory	Type	Description
description	No	String	Response description
schema	No	Object	Response body. For details, see Table 5-606 .

Table 5-606 Parameter description of schema

Parameter	Mandatory	Type	Description
description	No	String	Body description
type	No	String	Body type, which can be FORM or STREAM

Table 5-607 Parameter description of securityDefinitions

Parameter	Mandatory	Type	Description
name	Yes	Object	Security authentication mode. For details, see Table 5-608 .

Table 5-608 Parameter description of name

Parameter	Mandatory	Type	Description
type	Yes	String	Authentication type. apiKey is supported.
name	Yes	String	Name of apiKey
in	Yes	String	Location of apiKey
x-apigateway-auth-type	Yes	String	Authentication type extended based on apiKey. Authentication types AppSigv1, IAM, and IAM_NONE are supported.

Table 5-609 Parameter description of x-apigateway-backend

Parameter	Mandatory	Type	Description
type	Yes	String	Backend type. The options include HTTP , HTTP-VPC , FUNCTION , and MOCK .
parameters	No	Object	Backend parameters. For details, see backend parameter description .
backend_definition	Yes	Object	Backend definition The following backend definitions are supported: • httpEndpoints: See parameter description of backend httpEndpoints. • httpVpcEndpoints: See parameter description of backend httpVpcEndpoints. • functionEndpoints: See parameter description of backend functionEndpoints. • mockEndpoints: See parameter description of backend mockEndpoints.

Table 5-610 Parameter description of x-apigateway-backend-policies

Parameter	Mandatory	Type	Description
type	Yes	String	Backend type. The options include HTTP , HTTP-VPC , FUNCTION , and MOCK .
name	No	String	Backend policy name
parameters	No	Object	Backend parameters. For details, see backend parameter description .

Parameter	Mandatory	Type	Description
backend_definition	Yes	Object	Backend definition The following backend definitions are supported: • httpEndpoints: See parameter description of backend httpEndpoints. • httpVpcEndpoints: See parameter description of backend httpVpcEndpoints. • functionEndpoints: See parameter description of backend functionEndpoints. • mockEndpoints: See parameter description of backend mockEndpoints.
conditions	Yes	Object	Policy conditions. For details, see parameter description of conditions .
effectMode	Yes	String	Effective mode of the backend policy. The options include ANY and ALL .

Table 5-611 Backend parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name, which consists of a maximum of 32 bytes, starting with a letter. Only letters, digits, periods (.), hyphens (-), and underscores (_) are allowed. The names of header parameters are not case-sensitive.
value	Yes	String	Parameter value, which is a parameter name if the parameter comes from a request
in	Yes	String	Parameter location, which can be header , query , or path
origin	Yes	String	Parameter mapping source. The options include REQUEST and CONSTANT .
description	No	String	Parameter meaning

Table 5-612 Parameter description of backend httpEndpoints

Parameter	Mandatory	Type	Description
address	Yes	String	Backend service address. The format is <i><Domain name or IP address>:[Port number]</i>
scheme	Yes	String	Backend request protocol. HTTP and HTTPS are supported.
method	Yes	String	Backend request method. The options include GET, POST, PUT, DELETE, HEAD, OPTIONS, PATCH , and ANY .
path	Yes	String	Backend request path, which can contain variables.
timeout	No	Integer	Backend request timeout in milliseconds. The value ranges from 1 to 60,000, and the default value is 5000 .
description	No	String	Backend description

Table 5-613 Parameter description of backend httpVpcEndpoints

Parameter	Mandatory	Type	Description
name	Yes	Array	VPC channel name
scheme	Yes	String	Backend request protocol. HTTP and HTTPS are supported.
method	Yes	String	Backend request method. The options include GET, POST, PUT, DELETE, HEAD, OPTIONS, PATCH , and ANY .
path	Yes	String	Backend request path, which can contain variables.
timeout	No	Integer	Backend request timeout in milliseconds. The value ranges from 1 to 60,000, and the default value is 5000 .
host	No	String	VPC channel proxy host
description	No	String	Backend description

Table 5-614 Parameter description of backend functionEndpoints

Parameter	Mandatory	Type	Description
function-urn	Yes	String	Function URN
version	Yes	String	Function version
invocation-type	Yes	String	Function invocation type. The value can be async or sync .
timeout	No	Integer	Function timeout in milliseconds. The value ranges from 1 to 60,000, and the default value is 5000 .
description	No	String	Backend description

Table 5-615 Parameter description of backend mockEndpoints

Parameter	Mandatory	Type	Description
result-content	Yes	String	Mock response
description	No	String	Backend description

Table 5-616 Parameter description of conditions

Parameter	Mandatory	Type	Description
type	Yes	String	Policy condition type. The options include equal , enum , and pattern .
value	Yes	String	Policy condition value
origin	Yes	String	Policy condition source. The options include source and request .
parameter	No	String	Input parameter name if the origin parameter is set to request .

Table 5-617 Parameter description of x-apigateway-access-controls

Parameter	Mandatory	Type	Description
acl_name	No	Object	Access control policy. For details, see parameter description of acl_name .

Table 5-618 Parameter description of acl_name

Parameter	Mandatory	Type	Description
acl-type	Yes	String	Access control effect. The options include PERMIT and DENY .
entity-type	Yes	String	Access control object. Only IP addresses and accounts are supported.
value	Yes	String	Access control values, which are separated with commas (,).

Table 5-619 Parameter description of x-apigateway-ratelimits

Parameter	Mandatory	Type	Description
throttle_name	No	Object	Request throttling policy. For details, see parameter description of throttle_name .

Table 5-620 Parameter description of throttle_name

Parameter	Mandatory	Type	Description
api-limit	Yes	Integer	Maximum number of times an API can be called
user-limit	No	Integer	Number of times the API can be called by a user
app-limit	No	Integer	Number of times the API can be called by an app
ip-limit	No	Integer	Number of times the API can be called by an IP address
interval	Yes	Integer	Throttling period
unit	Yes	String	Throttling unit, which can be SECOND , MINUTE , HOURL , or DAY
shared	No	Boolean	Whether to share the throttling limits among APIs
special	No	Object	Excluded request throttling configurations. For details, see parameter description of special .

Table 5-621 Parameter description of special

Parameter	Mandatory	Type	Description
type	Yes	String	Excluded request throttling type, which can be APP or USER
limit	Yes	Integer	Access limit
instance	Yes	String	Excluded app or user

Example request:

```
{
  "swagger": "2.0",
  "info": {
    "description": "api group test",
    "title": "APIGroup_test",
    "version": "2019-09-12-17:38:10"
  },
  "paths": {
    "/test/{path}": {
      "get": {
        "security": [
          {
            "apig-auth-app": []
          }
        ],
        "description": "api test",
        "schemes": [
          "https"
        ],
        "operationId": "API_test",
        "parameters": [
          {
            "type": "string",
            "description": "header parameter",
            "name": "header",
            "in": "header",
            "required": true
          },
          {
            "type": "string",
            "description": "path parameter",
            "name": "path",
            "in": "path",
            "required": true
          },
          {
            "type": "number",
            "default": "123",
            "description": "query parameter",
            "name": "query",
            "in": "query"
          }
        ],
        "responses": {
          "default": {
            "$ref": "#/responses/default"
          },
          "x-apigateway-result-failure-sample": "",
          "x-apigateway-result-normal-sample": "success"
        }
      }
    }
  }
}
```

```
"x-apigateway-backend": {
  "httpEndpoints": {
    "address": "1.1.1.1:443",
    "description": "",
    "method": "GET",
    "path": "/test/{path}",
    "scheme": "https",
    "timeout": 5000
  },
  "parameters": [
    {
      "description": "",
      "in": "HEADER",
      "name": "header",
      "origin": "REQUEST",
      "value": "header"
    },
    {
      "description": "",
      "in": "PATH",
      "name": "path",
      "origin": "REQUEST",
      "value": "path"
    },
    {
      "description": "",
      "in": "QUERY",
      "name": "query",
      "origin": "REQUEST",
      "value": "query"
    }
  ],
  "type": "HTTP"
},
"x-apigateway-backend-policies": [
  {
    "conditions": [
      {
        "origin": "param",
        "parameter": "path",
        "type": "exact",
        "value": "path"
      },
      {
        "origin": "source",
        "parameter": "",
        "type": "",
        "value": "1.0.0.0/8"
      }
    ],
    "effectMode": "ANY",
    "httpVpcEndpoints": {
      "method": "POST",
      "name": "VPC_n9ct",
      "path": "/",
      "scheme": "HTTPS",
      "timeout": 5000
    },
    "name": "policy_test",
    "type": "HTTP-VPC"
  }
],
"x-apigateway-cors": false,
"x-apigateway-match-mode": "NORMAL",
"x-apigateway-request-type": "public"
}
},
"responses": {
```

```
{
  "default": {
    "description": "response example"
  },
  "securityDefinitions": {
    "apig-auth-app": {
      "type": "apiKey",
      "name": "Authorization",
      "in": "header",
      "x-apigateway-auth-type": "AppSigv1"
    },
    "apig-auth-iam": {
      "type": "apiKey",
      "name": "unused",
      "in": "header",
      "x-apigateway-auth-type": "IAM"
    }
  }
}
```

Response

Table 5-622 Parameter description

Parameter	Type	Description
group_id	String	API group ID
success	Array	Import success information
failure	Array	Import failure information

Table 5-623 Parameter description of success

Parameter	Type	Description
id	String	ID of a successfully imported API
action	String	Import type. Options: • update: Updates the APIs in an existing API group. • create: Creates APIs for a new API group.
method	String	Request method
path	String	Request path

Table 5-624 Parameter description of failure

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Parameter	Type	Description
method	String	Request method
path	String	Request path

Example response:

```
{
  "group_id": "27aa2317e3514c5bb5aab5587a5e50ea",
  "success": [
    {
      "id": "aea39194d8db46408be0174b0bd15931",
      "action": "create",
      "method": "GET",
      "path": "/test01"
    }
  ],
  "failure": [
    {
      "error_code": "APIG.2011",
      "error_msg": "Parameter value does not match the rules,parameterName:backend_type",
      "method": "GET",
      "path": "/test02"
    }
  ]
}
```

Status Codes

Table 5-625 Status codes

Status Code	Description
200	OK
400	Bad Request
403	Forbidden
500	Server Internal Error

5.20.4 Importing APIs to an Existing API Group

Function

This API is used to create or update APIs in an API group by importing Swagger definitions. Swagger files in JSON or YAML format are supported.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-626

Request Method	URI
PUT	/v1.0/apigw/openapi?group_id={0}&mode={1}

The following table lists the parameters in the URI.

Table 5-627 Parameter description

Parameter	Mandatory	Type	Description
group_id	Yes	String	API group ID
mode	Yes	String	Action to be taken if a conflict occurs. Options: merge and override . • merge: Retains the original API. • override: Overwrites the existing API.
extend_mode	No	String	Extended definition import mode. The options include merge and override . If the extended definition conflicts with existing API definition, you can choose to retain or override the existing definition.

Request

Table 5-628 Parameter description

Parameter	Mandatory	Type	Description
swagger	Yes	String	The value is fixed at 2.0 .
info	Yes	Object	See Table 5-629 .
paths	Yes	Object	See parameter description of paths .
responses	No	Object	Common response, which can be referenced in {method} . For details, see Table 5-634 .
securityDefinitions	Yes	Object	Security authentication mode definition. For details, see Table 5-638 .

Parameter	Mandatory	Type	Description
x-apigateway-access-controls	No	Object	Access control information. For details, see parameter description of x-apigateway-access-controls .
x-apigateway-ratelimits	No	Object	Request throttling information. For details, see parameter description of x-apigateway-ratelimits .

Table 5-629 Parameter description of info

Parameter	Mandatory	Type	Description
title	No	String	Name of an API group. This parameter does not take effect when the API group is imported to an existing group.
version	No	String	Version number. You can specify a version number or use the current date and time by default.
description	No	String	Description of the API group

Table 5-630 Parameter description of paths

Parameter	Mandatory	Type	Description
uri	Yes	Object	API access address. For details, see Table 5-631 .

Table 5-631 Parameter description of uri

Parameter	Mandatory	Type	Description
method	Yes	Object	API access method. For details, see Table 5-632 .

Table 5-632 Parameter description of method

Parameter	Mandatory	Type	Description
operationId	No	String	API name
description	No	String	API description
schemes	No	Object	API request protocol. HTTP and HTTPS are supported.
tags	No	Object	API tags
parameters	No	Object	Request parameter definitions. For details, see frontend parameter description .
responses	No	Object	Response definition. For details, see Table 5-634 .
security	No	Object	Security authentication mode. For details, see parameter description of security .
x-apigateway-access-control	No	Object	Access control policy bound to the API
x-apigateway-backend	No	Object	Backend information. For details, see parameter description of x-apigateway-backend .
x-apigateway-backend-policies	No	Object	Backend policy information. For details, see parameter description of x-apigateway-backend-policies .
x-apigateway-cors	No	Boolean	Indicates whether CORS is supported.
x-apigateway-match-mode	No	String	Route matching mode
x-apigateway-ratelimit	No	String	Name of the request throttling policy bound to the API
x-apigateway-request-type	No	String	API type

Table 5-633 Frontend parameter description

Parameter	Mandatory	Type	Description
maximum	No	Float	Maximum value of a number type parameter
minimum	No	Float	Minimum value of a number type parameter

Parameter	Mandatory	Type	Description
maxLength	No	Integer	Maximum length of a string type parameter
minLength	No	Integer	Minimum length of a string type parameter
pattern	No	String	Regular expression of the parameter value
type	No	String	Type
default	No	String	Default value
description	No	String	Parameter description
name	No	String	Parameter name
in	No	String	Parameter location, which can be path , header , query , formData , or body
required	No	Boolean	Whether the parameter is required. The parameter is required when its location is path .

Table 5-634 Parameter description of responses

Parameter	Mandatory	Type	Description
default	No	Object	Default response, which will be used when no status codes are defined
status_code	No	Object	Response status code. For details, see Table 5-636 .
x-apigateway-result-failure-sample	No	String	Example response for a failed request
x-apigateway-result-normal-sample	No	String	Example response for a successful request

Table 5-635 Parameter description of security

Parameter	Mandatory	Type	Description
apig-auth-type	No	Object	Security authentication mode. This parameter is a null array. Options: • apig-auth-app: App authentication • apig-auth-iam: IAM authentication • Null: No authentication required

Table 5-636 Parameter description of status_code

Parameter	Mandatory	Type	Description
description	No	String	Response description
schema	No	Object	Response body. For details, see Table 5-637 .

Table 5-637 Parameter description of schema

Parameter	Mandatory	Type	Description
description	No	String	Body description
type	No	String	Body type, which can be FORM or STREAM

Table 5-638 Parameter description of securityDefinitions

Parameter	Mandatory	Type	Description
name	Yes	Object	Security authentication mode. For details, see Table 5-639 .

Table 5-639 Parameter description of name

Parameter	Mandatory	Type	Description
type	Yes	String	Authentication type. apiKey is supported.

Parameter	Mandatory	Type	Description
name	Yes	String	Name of apiKey
in	Yes	String	Location of apiKey
x-apigateway-auth-type	Yes	String	Authentication type extended based on apiKey. Authentication types AppSigv1, IAM, and IAM_NONE are supported.

Table 5-640 Parameter description of x-apigateway-backend

Parameter	Mandatory	Type	Description
type	Yes	String	Backend type. The options include HTTP , HTTP-VPC , FUNCTION , and MOCK .
parameters	No	Object	Backend parameters. For details, see backend parameter description .
backend_definition	Yes	Object	Backend definition The following backend definitions are supported: • httpEndpoints: See parameter description of backend httpEndpoints. • httpVpcEndpoints: See parameter description of backend httpVpcEndpoints. • functionEndpoints: See parameter description of backend functionEndpoints. • mockEndpoints: See parameter description of backend mockEndpoints.

Table 5-641 Parameter description of x-apigateway-backend-policies

Parameter	Mandatory	Type	Description
type	Yes	String	Backend type. The options include HTTP , HTTP-VPC , FUNCTION , and MOCK .
name	No	String	Backend policy name

Parameter	Mandatory	Type	Description
parameters	No	Object	Backend parameters. For details, see backend parameter description .
backend_definition	Yes	Object	Backend definition The following backend definitions are supported: • httpEndpoints: See parameter description of backend httpEndpoints. • httpVpcEndpoints: See parameter description of backend httpVpcEndpoints. • functionEndpoints: See parameter description of backend functionEndpoints. • mockEndpoints: See parameter description of backend mockEndpoints.
conditions	Yes	Object	Policy conditions. For details, see parameter description of conditions .
effectMode	Yes	String	Effective mode of the backend policy. The options include ANY and ALL .

Table 5-642 Backend parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name, which consists of a maximum of 32 bytes, starting with a letter. Only letters, digits, periods (.), hyphens (-), and underscores (_) are allowed. The names of header parameters are not case-sensitive.
value	Yes	String	Parameter value, which is a parameter name if the parameter comes from a request
in	Yes	String	Parameter location, which can be header , query , or path
origin	Yes	String	Parameter mapping source. The options include REQUEST and CONSTANT .

Parameter	Mandatory	Type	Description
description	No	String	Parameter meaning

Table 5-643 Parameter description of backend httpEndpoints

Parameter	Mandatory	Type	Description
address	Yes	String	Backend service address. The format is <i><Domain name or IP address>:[Port number]</i>
scheme	Yes	String	Backend request protocol. HTTP and HTTPS are supported.
method	Yes	String	Backend request method. The options include GET , POST , PUT , DELETE , HEAD , OPTIONS , PATCH , and ANY .
path	Yes	String	Backend request path, which can contain variables.
timeout	No	Integer	Backend request timeout in milliseconds. The value ranges from 1 to 60,000, and the default value is 5000 .
description	No	String	Backend description

Table 5-644 Parameter description of backend httpVpcEndpoints

Parameter	Mandatory	Type	Description
name	Yes	Array	VPC channel name
scheme	Yes	String	Backend request protocol. HTTP and HTTPS are supported.
method	Yes	String	Backend request method. The options include GET , POST , PUT , DELETE , HEAD , OPTIONS , PATCH , and ANY .
path	Yes	String	Backend request path, which can contain variables.
timeout	No	Integer	Backend request timeout in milliseconds. The value ranges from 1 to 60,000, and the default value is 5000 .
host	No	String	VPC channel proxy host

Parameter	Mandatory	Type	Description
description	No	String	Backend description

Table 5-645 Parameter description of backend functionEndpoints

Parameter	Mandatory	Type	Description
function-urn	Yes	String	Function URN
version	Yes	String	Function version
invocation-type	Yes	String	Function invocation type. The value can be async or sync .
timeout	No	Integer	Function timeout in milliseconds. The value ranges from 1 to 60,000, and the default value is 5000 .
description	No	String	Backend description

Table 5-646 Parameter description of backend mockEndpoints

Parameter	Mandatory	Type	Description
result-content	Yes	String	Mock response
description	No	String	Backend description

Table 5-647 Parameter description of conditions

Parameter	Mandatory	Type	Description
type	Yes	String	Policy condition type. The options include equal , enum , and pattern .
value	Yes	String	Policy condition value
origin	Yes	String	Policy condition source. The options include source and request .
parameter	No	String	Input parameter name if the origin parameter is set to request .

Table 5-648 Parameter description of x-apigateway-access-controls

Parameter	Mandatory	Type	Description
acl_name	No	Object	Access control policy. For details, see parameter description of acl_name .

Table 5-649 Parameter description of acl_name

Parameter	Mandatory	Type	Description
acl-type	Yes	String	Access control effect. The options include PERMIT and DENY .
entity-type	Yes	String	Access control object. Only IP addresses and accounts are supported.
value	Yes	String	Access control values, which are separated with commas (,).

Table 5-650 Parameter description of x-apigateway-ratelimits

Parameter	Mandatory	Type	Description
throttle_name	No	Object	Request throttling policy. For details, see parameter description of throttle_name .

Table 5-651 Parameter description of throttle_name

Parameter	Mandatory	Type	Description
api-limit	Yes	Integer	Maximum number of times an API can be called
user-limit	No	Integer	Number of times the API can be called by a user
app-limit	No	Integer	Number of times the API can be called by an app
ip-limit	No	Integer	Number of times the API can be called by an IP address
interval	Yes	Integer	Throttling period

Parameter	Mandatory	Type	Description
unit	Yes	String	Throttling unit, which can be SECOND , MINUTE , HOURL , or DAY
shared	No	Boolean	Whether to share the throttling limits among APIs
special	No	Object	Excluded request throttling configurations. For details, see parameter description of special .

Table 5-652 Parameter description of special

Parameter	Mandatory	Type	Description
type	Yes	String	Excluded request throttling type, which can be APP or USER
limit	Yes	Integer	Access limit
instance	Yes	String	Excluded app or user

Example request:

```
{
  "swagger": "2.0",
  "info": {
    "description": "api group test",
    "title": "APIGroup_test",
    "version": "2019-09-12-17:38:10"
  },
  "paths": {
    "/test/{path}": {
      "get": {
        "security": [
          {
            "apig-auth-app": []
          }
        ],
        "description": "api test",
        "schemes": [
          "https"
        ],
        "operationId": "API_test",
        "parameters": [
          {
            "type": "string",
            "description": "header parameter",
            "name": "header",
            "in": "header",
            "required": true
          },
          {
            "type": "string",
            "description": "path parameter",
```

```
        "name": "path",
        "in": "path",
        "required": true
      },
      {
        "type": "number",
        "default": "123",
        "description": "query parameter",
        "name": "query",
        "in": "query"
      }
    ],
    "responses": {
      "default": {
        "$ref": "#/responses/default"
      },
      "x-apigateway-result-failure-sample": "",
      "x-apigateway-result-normal-sample": "success"
    },
    "x-apigateway-backend": {
      "httpEndpoints": {
        "address": "1.1.1.1:443",
        "description": "",
        "method": "GET",
        "path": "/test/{path}",
        "scheme": "https",
        "timeout": 5000
      },
      "parameters": [
        {
          "description": "",
          "in": "HEADER",
          "name": "header",
          "origin": "REQUEST",
          "value": "header"
        },
        {
          "description": "",
          "in": "PATH",
          "name": "path",
          "origin": "REQUEST",
          "value": "path"
        },
        {
          "description": "",
          "in": "QUERY",
          "name": "query",
          "origin": "REQUEST",
          "value": "query"
        }
      ],
      "type": "HTTP"
    },
    "x-apigateway-backend-policies": [
      {
        "conditions": [
          {
            "origin": "param",
            "parameter": "path",
            "type": "exact",
            "value": "path"
          },
          {
            "origin": "source",
            "parameter": "",
            "type": "",
            "value": "1.0.0.0/8"
          }
        ]
      }
    ],
  ],
}
```

```
        "effectMode": "ANY",
        "httpVpcEndpoints": {
            "method": "POST",
            "name": "VPC_n9ct",
            "path": "/",
            "scheme": "HTTPS",
            "timeout": 5000
        },
        "name": "policy_test",
        "type": "HTTP-VPC"
    },
    ],
    "x-apigateway-cors": false,
    "x-apigateway-match-mode": "NORMAL",
    "x-apigateway-request-type": "public"
}
}
},
"responses": {
    "default": {
        "description": "response example"
    }
},
"securityDefinitions": {
    "apig-auth-app": {
        "type": "apiKey",
        "name": "Authorization",
        "in": "header",
        "x-apigateway-auth-type": "AppSigv1"
    },
    "apig-auth-iam": {
        "type": "apiKey",
        "name": "unused",
        "in": "header",
        "x-apigateway-auth-type": "IAM"
    }
}
}
```

Response

Table 5-653 Parameter description

Parameter	Type	Description
group_id	String	API group ID
success	Array	Import success information
failure	Array	Import failure information

Table 5-654 Parameter description of success

Parameter	Type	Description
id	String	ID of a successfully imported API

Parameter	Type	Description
action	String	Import type. Options: • update: Updates the APIs in an existing API group. • create: Creates APIs for a new API group.
method	String	Request method
path	String	Request path

Table 5-655 Parameter description of failure

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
method	String	Request method
path	String	Request path

Example response:

```
{
  "group_id": "27aa2317e3514c5bb5aab5587a5e50ea",
  "success": [
    {
      "id": "aea39194d8db46408be0174b0bd15931",
      "action": "create",
      "method": "GET",
      "path": "/test01"
    }
  ],
  "failure": [
    {
      "error_code": "APIG.2011",
      "error_msg": "Parameter value does not match the rules,parameterName:backend_type",
      "method": "GET",
      "path": "/test02"
    }
  ]
}
```

Status Codes

Table 5-656 Status codes

Status Code	Description
200	OK
400	Bad Request

Status Code	Description
403	Forbidden
500	Server Internal Error

5.21 Custom Authorizer Management

5.21.1 Creating a Custom Authorizer

Function

This API is used to create a custom authorizer.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-657 HTTP/HTTPS request method and URI

Request Method	URI
POST	/v1.0/apigw/authorizers

Request

Table 5-658 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	Name of a custom authorizer The name of a custom authorizer consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.
type	Yes	String	Type of the custom authorizer, which can be: • FRONTEND • BACKEND
authorizer_type	Yes	String	Value: FUNC

Parameter	Mandatory	Type	Description
authorizer_uri	Yes	String	Function URN
identities	No	List	Certification source
ttl	No	Integer	Cache duration
user_data	No	String	User data

Table 5-659 Parameter description of identities

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name
location	Yes	String	Parameter location, which can be: • HEADER • QUERY

Example request:

```
{
  "name": "Authorizer_9dlh",
  "type": "FRONTEND",
  "authorizer_type": "FUNC",
  "authorizer_uri": "urn:fss:regionexample:dbb5762c88f045c6a1427a952bcae284:function:default:test111",
  "ttl": 10,
  "user_data": "aaaa",
  "identities": [
    {
      "name": "Authorization",
      "location": "HEADER"
    }
  ]
}
```

Response

Table 5-660 Parameter description

Parameter	Type	Description
id	String	ID of the custom authorizer
name	String	Name of the custom authorizer
type	String	Type of the custom authorizer, which can be: • FRONTEND • BACKEND

Parameter	Type	Description
authorizer_type	String	Value: FUNC
authorizer_uri	String	Function URN
identities	Array	Certification source
ttl	Integer	Cache duration
user_data	String	User data
create_time	Time	Time when the custom authorizer is created

Table 5-661 Parameter description of identities

Parameter	Type	Description
name	String	Parameter name
location	String	Parameter location, which can be: • HEADER • QUERY

Example response:

```
{
  "name": "Authorizer_9dlh",
  "type": "FRONTEND",
  "authorizer_type": "FUNC",
  "authorizer_uri": "urn:fss:regionexample:dbb5762c88f045c6a1427a952bcae284:function:default:test111",
  "identities": [
    {
      "name": "Authorization",
      "location": "HEADER",
    }
  ],
  "ttl": 10,
  "user_data": "aaaa",
  "id": "7345e3fe4047491ebd8ecb0acd665a4c",
  "create_time": "2020-01-19T11:48:56.576611862Z"
}
```

Status Codes

Table 5-662 Status codes

Status Code	Description
201	Created
400	Bad Request

Status Code	Description
401	Unauthorized
403	Forbidden
500	Server Internal Error

5.21.2 Modifying a Custom Authorizer

Function

This API is used to modify a specified custom authorizer.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-663 HTTP/HTTPS request method and URI

Request Method	URI
PUT	/v1.0/apigw/authorizers/{id}

The following table lists the parameter in the URI.

Table 5-664 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	ID of a custom authorizer

Request

Table 5-665 Parameter description

Parameter	Mandatory	Type	Description
name	Yes	String	Name of the custom authorizer The name of a custom authorizer consists of 3–64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.

Parameter	Mandatory	Type	Description
type	Yes	String	Type of the custom authorizer, which can be: • FRONTEND • BACKEND
authorizer_type	Yes	String	Value: FUNC
authorizer_uri	Yes	String	Function URN
identities	No	List	Certification source
ttl	No	Integer	Cache duration
user_data	No	String	User data

Table 5-666 Parameter description of identities

Parameter	Mandatory	Type	Description
name	Yes	String	Parameter name
location	Yes	String	Parameter location, which can be: • HEADER • QUERY

Example request:

```
{
  "name": "Authorizer_9dlh",
  "type": "FRONTEND",
  "authorizer_type": "FUNC",
  "authorizer_uri": "urn:fss:regionexample:dbb5762c88f045c6a1427a952bcae284:function:default:test111",
  "ttl": 10,
  "user_data": "aaaa",
  "identities": [
    {
      "name": "Authorization",
      "location": "HEADER"
    }
  ]
}
```

Response

Table 5-667 Parameter description

Parameter	Type	Description
id	String	ID of the custom authorizer
name	String	Name of the custom authorizer
type	String	Type of the custom authorizer, which can be: • FRONTEND • BACKEND
authorizer_type	String	Value: FUNC
authorizer_uri	String	Function URN
identities	Array	Certification source
ttl	Integer	Cache duration
user_data	String	User data
create_time	Time	Time when the custom authorizer is created

Table 5-668 Parameter description of identities

Parameter	Type	Description
name	String	Parameter name
location	String	Parameter location, which can be: • HEADER • QUERY

Example response:

```
{
  "name": "Authorizer_9dlh",
  "type": "FRONTEND",
  "authorizer_type": "FUNC",
  "authorizer_uri": "urn:fss:regionexample:dbb5762c88f045c6a1427a952bcae284:function:default:test111",
  "identities": [
    {
      "name": "Authorization",
      "location": "HEADER",
    }
  ],
  "ttl": 10,
  "user_data": "aaaa",
  "id": "7345e3fe4047491ebd8ecb0acd665a4c",
  "create_time": "2020-01-19T11:48:56.576611862Z"
}
```

Status Codes

Table 5-669 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
500	Server Internal Error

5.21.3 Deleting a Custom Authorizer

Function

This API is used to delete a specified custom authorizer.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-670 HTTP/HTTPS request method and URI

Request Method	URI
DELETE	/v1.0/apigw/authorizers/{id}

The following table lists the parameter in the URI.

Table 5-671 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	ID of a custom authorizer

Request

N/A

Response

N/A

Status Codes

Table 5-672 Status codes

Status Code	Description
204	No Content
401	Unauthorized
403	Forbidden
404	Not Found
409	Conflict
500	Server Internal Error

5.21.4 Querying Details of a Custom Authorizer

Function

This API is used to query the details of a specified custom authorizer.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-673 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/authorizers/{id}

The following table lists the parameters in the URI.

Table 5-674 Parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	ID of a custom authorizer

Request

N/A

Response

Table 5-675 Parameter description

Parameter	Type	Description
id	String	ID of the custom authorizer
name	String	Name of the custom authorizer
type	String	Type of the custom authorizer, which can be: • FRONTEND • BACKEND
authorizer_type	String	Value: FUNC
authorizer_uri	String	Function URN
identities	Array	Certification source
ttl	Integer	Cache duration
user_data	String	User data
create_time	Time	Time when the custom authorizer is created

Table 5-676 Parameter description of identities

Parameter	Type	Description
name	String	Parameter name
location	String	Parameter location, which can be: • HEADER • QUERY

Example response:

```
{
  "name": "Authorizer_9dlh",
  "type": "FRONTEND",
  "authorizer_type": "FUNC",
  "authorizer_uri": "urn:fss:regionexample:dbb5762c88f045c6a1427a952bcae284:function:default:test111",
  "identities": [
    {
      "name": "Authorization",
      "location": "HEADER",
    }
  ],
  "ttl": 10,
  "user_data": "aaaa",
  "id": "7345e3fe4047491ebd8ecb0acd665a4c",
  "create_time": "2020-01-19T11:48:56.576611862Z"
}
```

Status Codes

Table 5-677 Status codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
500	Server Internal Error

5.21.5 Querying a Custom Authorizer List

Function

This API is used to query a list of custom authorizers that match specified conditions.

URI

The following table lists the HTTP/HTTPS request method and URI of the API.

Table 5-678 HTTP/HTTPS request method and URI

Request Method	URI
GET	/v1.0/apigw/authorizers[?page_size, page_no, id, name, type]

NOTE

- A combination of different query conditions can be added at the end of the URI by using question marks (?) and ampersands (&).
- Query conditions include: **id**, **name**, **type**, **page_size**, and **page_no**.

The following table lists the parameters in the URI.

Table 5-679 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	ID of a custom authorizer

Parameter	Mandatory	Type	Description
name	No	String	Name of the custom authorizer
type	No	String	Type of the custom authorizer
page_size	No	Integer	Number of records displayed on each page. The default value is 20 .
page_no	No	Integer	Page number. The default value is 1 .

Request

N/A

Response

Table 5-680 Parameter description

Parameter	Type	Description
total	Integer	Number of custom authorizers that match the query conditions
size	Integer	Length of the returned custom authorizer list
authorizer_list	Array	Custom authorizer list

Table 5-681 Parameter description of authorizer_list

Parameter	Type	Description
id	String	ID of the custom authorizer
name	String	Name of the custom authorizer
type	String	Type of the custom authorizer, which can be: • FRONTEND • BACKEND
authorizer_type	String	Value: FUNC
authorizer_uri	String	Function URN

Parameter	Type	Description
identities	Array	Certification source
ttl	Integer	Cache duration
user_data	String	User data
create_time	Time	Time when the custom authorizer is created

Table 5-682 Parameter description of identities

Parameter	Type	Description
name	String	Parameter name
location	String	Parameter location, which can be: • HEADER • QUERY

Example response:

```
{
  "total":1,
  "size":1,
  "authorizer_list":[
    {
      "name":"Authorizer_9dlh",
      "type":"FRONTEND",
      "authorizer_type":"FUNC",
      "authorizer_uri":"urn:fss:regionexample:dbb5762c88f045c6a1427a952bcae284:function:default:test111",
      "identities":[
        {
          "name":"Authorization",
          "location":"HEADER",
        }
      ],
      "ttl":10,
      "user_data":"aaaa",
      "id":"7345e3fe4047491ebd8ecb0acd665a4c",
      "create_time":"2020-01-19T11:48:56Z"
    }
  ]
}
```

Status Codes

Table 5-683 Status codes

Status Code	Description
201	Created
400	Bad Request

Status Code	Description
401	Unauthorized
403	Forbidden
500	Server Internal Error

6 Permissions Policies and Supported Actions

This chapter describes fine-grained permissions management for your APIG.

NOTE

- If your Huawei Cloud account does not require individual IAM users, skip this section.
- Only **dedicated** gateways support fine-grained permissions management.

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles (in JSON format) to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions. For more information about policy syntax and for example policies, see [Creating a User and Granting APIG Permissions](#).

An account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions. The permissions required for calling an API are determined by the actions supported by the API. Only IAM users who have been granted permissions allowing the actions can call the API successfully. For example, if an IAM user wants to create APIs using an API, the user must have been granted permissions that allow the **apig:apis:create** action.

Supported Actions

Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- **Permission:** A statement in a policy that allows or denies certain operations.
- **Action:** Specific operations that are allowed or denied.
- **API:** REST APIs that can be called by a user who has been granted specific permissions.
- **Authorization scope:** Type of projects in which policies can be used to grant permissions. A policy can be applied to IAM projects, enterprise projects, or both. Policies that contain actions for both IAM and enterprise projects can be used and take effect for both IAM and Enterprise Management. Policies that only contain actions for IAM projects can be used and only take effect for

IAM. For details, see [What Are the Differences Between IAM Projects and Enterprise Projects?](#)

APIG supports actions that can be defined in custom policies. Permissions must be obtained before calling APIs provided by APIG. For details on how to obtain permissions, visit the [Identity and Access Management help center](#).

Table 6-1 Supported actions

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proj ect
Creating a dedicate d gateway	POST /v2/{project_id}/apigw/instances	apig:instances:create	-	√	√
Deleting a dedicate d gateway	DELETE /v2/{project_id}/apigw/instances/{instance_id}	apig:instances:delete	-	√	√
Updating a dedicate d gateway	PUT /v2/{project_id}/apigw/instances/{instance_id}	apig:instances:update	-	√	√
Querying details of a dedicate d gateway	GET /v2/{project_id}/apigw/instances/{instance_id}	apig:instances:get	-	√	√
Querying dedicate d gateways	GET /v2/{project_id}/apigw/instances	apig:instances:list	-	√	√
Querying domain names bound with a custom inbound port	GET /V2/{project_id}/apigw/instances/{instance_id}/custom-ingress-ports/{ingress_port_id}/domains	apig:instance:listCustomIngressPortDomain	apig:groups:get apig:instance:listCustomIngressPort apig:instances:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Querying custom inbound ports of a gateway	GET /V2/{project_id}/apigw/ instances/{instance_id}/ custom-ingress-ports	apig:insta nce:listCus tomIngres sPort	apig:instance s:get	√	√
Adding a custom inbound port	POST /V2/{project_id}/apigw/ instances/{instance_id}/ custom-ingress-ports	apig:insta nce:addCu stomIngres ssPort	apig:instance s:get	√	√
Deleting a custom inbound port	DELETE /V2/{project_id}/apigw/ instances/{instance_id}/ custom-ingress-ports/ {ingress_port_id}	apig:insta nce:delete CustomIn gressPort	apig:instance :listCustomIn gressPort apig:instance s:get	√	√
Querying gateway s by tag	POST /V2/{project_id}/apigw/ resource-instances/filter	apig:insta nce:listByT ags	-	√	x
Querying the number of gateway s by tag	POST /V2/{project_id}/apigw/ resource-instances/count	apig:insta nce:getNu mByTags	-	√	x
Querying tags of a gateway	GET /v2/{project_id}/ apigw/instance-tags	apig:insta nceTags:lis t	-	√	x
Deleting tags of a gateway	POST /v2/{project_id}/ apigw/instances/ {instance_id}/instance- tags/action	apig:insta nceTags:d elete	apig:instance s:get	√	√
Creating a gateway tag	POST /V2/{project_id}/apigw/ instances/{instance_id}/ instance-tags/action	apig:insta nceTags:cr eate	apig:instance s:get	√	√
Creating an API group	POST /v2/{project_id}/ apigw/instances/ {instance_id}/api-groups	apig:group s:create	apig:instance s:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Deleting an API group	DELETE /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}	apig:group s:delete	apig:instance s:get	√	√
Querying details of an API group	GET /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}	apig:group s:get	apig:instance s:get	√	√
Querying API groups	GET /v2/{project_id}/apigw/instances/{instance_id}/api-groups	apig:group s:list	apig:instance s:get	√	√
Updating an API group	PUT /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}	apig:group s:update	apig:instance s:get	√	√
Binding a domain name to an API group	POST /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains	apig:doma ins:create	apig:instance s:get apig:groups: get	√	√
Unbinding a domain name from an API group	DELETE /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}	apig:doma ins:delete	apig:instance s:get apig:groups: get	√	√
Adding a certificate to a domain name	POST /v2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate	apig:doma ins:bindCe rtificate	apig:instance s:get apig:groups: get apig:domain s:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Deleting a certificate of a domain name	DELETE /v2/{project_id}/apigw/ instances/{instance_id}/ api-groups/{group_id}/ domains/{domain_id}/ certificate/{certificate_id}	apig:domains:unbind Certificate	apig:instances:get apig:groups: get apig:domains:get	√	√
Querying details of a certificate bound to a domain name	GET /v2/{project_id}/apigw/ instances/{instance_id}/ api-groups/{group_id}/ domains/{domain_id}/ certificate/{certificate_id}	apig:domains:getCertificate	apig:instances:get apig:groups: get apig:domains:get	√	√
Setting accessibility of a debugging domain name	PUT /v2/{project_id}/ apigw/instances/ {instance_id}/api-groups/ {group_id}/sl-domain- access-settings	apig:domains:update SLDomain Setting	apig:instances:get apig:groups: get	√	√
Creating an environment variable	POST /v2/{project_id}/apigw/ instances/{instance_id}/ env-variables	apig:variables:create	apig:instances:get apig:groups: get apig:envs:list	√	√
Deleting an environment variable	DELETE /v2/{project_id}/apigw/ instances/{instance_id}/ env-variables/ {env_variable_id}	apig:variables:delete	apig:instances:get apig:groups: get apig:envs:list	√	√
Querying details of an environment variable	GET /v2/{project_id}/apigw/ instances/{instance_id}/ env-variables/ {env_variable_id}	apig:variables:get	apig:instances:get apig:groups: get apig:envs:list	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Querying environ ment variables	GET /v2/{project_id}/apigw/instances/{instance_id}/env-variables	apig:variables:list	apig:instances:get apig:groups:get apig:envs:list	√	√
Creating an API	POST /v2/{project_id}/apigw/instances/{instance_id}/apis	apig:apis:create	apig:instances:get apig:groups:get	√	√
Deleting an API	DELETE /v2/{project_id}/apigw/instances/{instance_id}/apis/{api_id}	apig:apis:delete	apig:instances:get apig:groups:get	√	√
Publishing an API	POST /v2/{project_id}/apigw/instances/{instance_id}/apis/action	apig:apis:publish	apig:instances:get apig:groups:get apig:envs:list	√	√
Taking an API offline	POST /v2/{project_id}/apigw/instances/{instance_id}/apis/action	apig:apis:offline	apig:instances:get apig:groups:get apig:envs:list	√	√
Debugging an API	POST /v2/{project_id}/apigw/instances/{instance_id}/apis/debug/{api_id}	apig:apis:debug	apig:instances:get apig:groups:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Importin g an API	POST /v2/{project_id}/ apigw/instances/ {instance_id}/openapi/ import	apig:apis:i mport	apig:instance s:get apig:apis:cre ate apig:apis:bin dAcls apig:apis:bin dThrottles apig:groups: get apig:acls:cre ate apig:throttle s:create	√	√
Exportin g an API	POST /v2/{project_id}/ apigw/instances/ {instance_id}/openapi/ export	apig:apis:e xport	apig:instance s:get apig:apis:list apig:apis:get apig:apis:list BindedTrottl es apig:apis:list BindedAcls apig:groups: get apig:acls:get apig:throttle s:get	√	√
Updating an API	PUT /V2/{project_id}/apigw/ instances/{instance_id}/ apis/{api_id}	apig:apis:u pdate	apig:instance s:get apig:groups: get	√	√
Authorizi ng access to an API	POST /v2/{project_id}/ apigw/instances/ {instance_id}/app-auths	apig:apis:g rantAppAc cess	apig:instance s:get apig:apps:ge t apig:apis:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Cancelin g access authoriz ation for an API	DELETE /v2/{project_id}/ apigw/instances/ {instance_id}/app-auths/ {app_auth_id}	apig:apis:r elieveApp Access	apig:instance s:get apig:apps:ge t apig:apis:get	√	√
Binding a signature key to an API	POST /v2/{project_id}/ apigw/instances/ {instance_id}/sign- bindings	apig:apis:b indSigns	apig:instance s:get apig:apis:get apig:signs:list	√	√
Unbindin g a signature key from an API	DELETE /v2/{project_id}/ apigw/instances/ {instance_id}/sign- bindings/ {sign_bindings_id}	apig:apis:u nbindSign s	apig:instance s:get apig:apis:get apig:signs:list	√	√
Binding an access control policy to an API	POST /v2/{project_id}/ apigw/instances/ {instance_id}/acl-bindings	apig:apis:b indAcls	apig:instance s:get apig:apis:get apig:acls:get	√	√
Unbindin g an access control policy from an API	DELETE /v2/{project_id}/ apigw/instances/ {instance_id}/acl- bindings/ {acl_bindings_id}	apig:apis:u nbindAcls	apig:instance s:get apig:apis:get apig:acls:get	√	√
Binding a request throttlin g policy to an API	POST /v2/{project_id}/ apigw/instances/ {instance_id}/throttle- bindings	apig:apis:b indThrottl es	apig:instance s:get apig:apis:get apig:throttle s:get	√	√
Unbindin g a request throttlin g policy from an API	DELETE /v2/{project_id}/ apigw/instances/ {instance_id}/throttle- bindings/ {throttle_binding_id}	apig:apis:u nbindThro ttles	apig:instance s:get apig:apis:get apig:throttle s:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Querying details of an API	GET /v2/{project_id}/apigw/instances/{instance_id}/apis/{api_id}	apig:apis:get	apig:instances:get apig:groups:get	√	√
Querying APIs	GET /v2/{project_id}/apigw/instances/{instance_id}/apis	apig:apis:list	apig:instances:get apig:groups:get	√	√
Querying apps bound to an API	GET /v2/{project_id}/apigw/instances/{instance_id}/app-auths/binded-apps	apig:apis:listBindedApps	apig:instances:get apig:apis:get	√	√
Querying signature keys bound to an API	GET /v2/{project_id}/apigw/instances/{instance_id}/sign-bindings/binded-signs	apig:apis:listBindedSigns	apig:instances:get apig:apis:get	√	√
Querying access control policies bound to an API	GET /v2/{project_id}/apigw/instances/{instance_id}/acl-bindings/binded-acls	apig:apis:listBindedAcls	apig:instances:get apig:apis:get	√	√
Querying request throttling policies bound to an API	GET /v2/{project_id}/apigw/instances/{instance_id}/throttle-bindings/binded-throttles	apig:apis:listBindedThrottles	apig:instances:get apig:apis:get	√	√
Querying plug-ins bound with an API	GET /v2/{project_id}/apigw/instances/{instance_id}/apis/{api_id}/attached-plugins	apig:apis:listBindedPlugins	apig:instances:get apig:apis:get	√	√
Binding a plug-in to an API	POST /v2/{project_id}/apigw/instances/{instance_id}/apis/{api_id}/plugins/attach	apig:apis:bindPlugins	apig:instances:get apig:plugins:get apig:apis:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Unbindin g an API's plug-ins	PUT /v2/{project_id}/ apigw/instances/ {instance_id}/plugins/ {plugin_id}/detach	apig:apis:u nbindPlugi ns	apig:instance s:get apig:plugins: get apig:apis:get	√	√
Creating an environ ment	POST /v2/{project_id}/ apigw/instances/ {instance_id}/envs	apig:envs: create	apig:instance s:get	√	√
Deleting an environ ment	DELETE /v2/{project_id}/ apigw/instances/ {instance_id}/envs/ {env_id}	apig:envs: delete	apig:instance s:get	√	√
Querying environ ments	GET /v2/{project_id}/ apigw/instances/ {instance_id}/envs	apig:envs:l ist	apig:instance s:get	√	√
Updating an environ ment	PUT /V2/{project_id}/apigw/ instances/{instance_id}/ envs/{env_id}	apig:envs: update	apig:instance s:get	√	√
Creating an app	POST /v2/{project_id}/ apigw/instances/ {instance_id}/apps	apig:apps: create	apig:instance s:get	√	√
Deleting an app	DELETE /v2/{project_id}/ apigw/instances/ {instance_id}/apps/ {app_id}	apig:apps: delete	apig:instance s:get	√	√
Querying details of an app	GET /v2/{project_id}/ apigw/instances/ {instance_id}/apps/ {app_id}	apig:apps: get	apig:instance s:get	√	√
Querying apps	GET /v2/{project_id}/ apigw/instances/ {instance_id}/apps	apig:apps:l ist	apig:instance s:get	√	√
Querying APIs bound with an app	GET /v2/{project_id}/ apigw/instances/ {instance_id}/app-auths/ binded-apis	apig:apps:l istBindedA pis	apig:instance s:get apig:apps:ge t	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Querying APIs not bound with an app	GET /v2/{project_id}/apigw/instances/{instance_id}/app-auths/unbinded-apis	apig:apps:listUnbind edApis	apig:instance s:get apig:apps:ge t	√	√
Updating an applicati on	PUT /V2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}	apig:apps: update	apig:instance s:get	√	√
Creating a signature key	POST /v2/{project_id}/apigw/instances/{instance_id}/signs	apig:signs: create	apig:instance s:get	√	√
Deleting a signature key	DELETE /v2/{project_id}/apigw/instances/{instance_id}/signs/{sign_id}	apig:signs: delete	apig:instance s:get	√	√
Querying signature keys	GET /v2/{project_id}/apigw/instances/{instance_id}/signs	apig:signs: list	apig:instance s:get	√	√
Querying APIs bound with a signature key	GET /v2/{project_id}/apigw/instances/{instance_id}/sign-bindings/binded-apis	apig:signs: listBinded Apis	apig:instance s:get apig:signs:list	√	√
Querying APIs not bound with a signature key	GET /v2/{project_id}/apigw/instances/{instance_id}/sign-bindings/unbinded-apis	apig:signs: listUnbind edApis	apig:instance s:get apig:signs:list	√	√
Updating a signature key	PUT /V2/{project_id}/apigw/instances/{instance_id}/signs/{sign_id}	apig:signs: update	apig:instance s:get	√	√
Creating an access control policy	POST /v2/{project_id}/apigw/instances/{instance_id}/acls	apig:acls:c reate	apig:instance s:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Deleting an access control policy	DELETE /v2/{project_id}/apigw/instances/{instance_id}/acls/{acl_id}	apig:acls:delete	apig:instances:get	√	√
Querying details of an access control policy	GET /v2/{project_id}/apigw/instances/{instance_id}/acls/{acl_id}	apig:acls:get	apig:instances:get	√	√
Querying access control policies	GET /v2/{project_id}/apigw/instances/{instance_id}/acls	apig:acls:list	apig:instances:get	√	√
Querying APIs bound with an access control policy	GET /v2/{project_id}/apigw/instances/{instance_id}/acl-bindings/binded-apis	apig:acl:listBoundApi	apig:instances:get apig:acls:get	√	√
Querying APIs not bound with an access control policy	GET /v2/{project_id}/apigw/instances/{instance_id}/acl-bindings/unbinded-apis	apig:acls:listUnbindedApis	apig:instances:get apig:acls:get	√	√
Updating an access control policy	PUT /v2/{project_id}/apigw/instances/{instance_id}/acls/{acl_id}	apig:acls:update	apig:instances:get	√	√
Creating a request throttling policy	POST /v2/{project_id}/apigw/instances/{instance_id}/throttles	apig:throttles:create	apig:instances:get	√	√
Deleting a request throttling policy	DELETE /v2/{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}	apig:throttles:delete	apig:instances:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Querying details of a request throttling policy	GET /v2/{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}	apig:specialThrottles:get	apig:instances:get	√	√
Querying request control policies	GET /v2/{project_id}/apigw/instances/{instance_id}/throttles	apig:throttles:list	apig:instances:get	√	√
Querying APIs bound with a request throttling policy	GET /v2/{project_id}/apigw/instances/{instance_id}/throttle-bindings/binded-apis	apig:throttles:listBindedApis	apig:instances:get apig:throttles:get	√	√
Querying APIs not bound with a request throttling policy	GET /v2/{project_id}/apigw/instances/{instance_id}/throttle-bindings/unbinded-apis	apig:throttles:listUnbindedApis	apig:instances:get apig:throttles:get	√	√
Updating a request throttling policy	PUT /v2/{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}	apig:throttles:update	apig:instances:get	√	√
Creating an excluded request throttling configuration	POST /v2/{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials	apig:specialThrottles:create	apig:instances:get apig:throttles:get	√	√
Deleting an excluded request throttling configuration	DELETE /v2/{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials/{strategy_id}	apig:specialThrottles:delete	apig:instances:get apig:throttles:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Querying excluded request throttling configurations	GET /v2/{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials	apig:specialThrottles:get	apig:instances:get apig:throttles:get	√	√
Updating an excluded request throttling configuration	PUT /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials/{strategy_id}	apig:specialThrottles:update	apig:instances:get apig:throttles:get	√	√
Creating a load balance channel	POST /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels	apig:vpcChannels:create	apig:instances:get	√	√
Deleting a load balance channel	DELETE /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}	apig:vpcChannels:delete	apig:instances:get	√	√
Updating a load balance channel	PUT /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}	apig:vpcChannels:update	apig:instances:get	√	√
Adding a backend instance to a load balance channel	POST /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members	apig:vpcChannels:addInstance	apig:instances:get apig:vpcChannels:get	√	√
Deleting a backend instance	DELETE /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/{member_id}	apig:vpcChannels:deleteInstance	apig:instances:get apig:vpcChannels:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Querying load balance channel details	GET /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}	apig:vpcChannels:get	apig:instances:get	√	√
Querying load balance channels	GET /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels	apig:vpcChannels:list	apig:instances:get	√	√
Updating a backend server group of a VPC channel	PUT /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}	apig:vpcChannels:updateMemberGroup	apig:instances:get apig:vpcChannels:get	√	√
Adding or updating a backend server group of a VPC channel	POST /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups	apig:vpcChannels:addOrUpdateMemberGroups	apig:instances:get apig:vpcChannels:get	√	√
Disabling backend servers	POST /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/batch-disable	apig:vpcChannels:batchEnableInstance	apig:instances:get apig:vpcChannels:get	√	√
Deleting a backend server group of a VPC channel	DELETE /v2/{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}	apig:vpcChannels:deleteMemberGroup	apig:instances:get apig:vpcChannels:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Enabling backend servers	POST /v2/{project_id}/ apigw/instances/ {instance_id}/vpc- channels/ {vpc_channel_id}/ members/batch-enable	apig:vpcC hannels:b atchDisabl eInstance	apig:instance s:get apig:vpcCha nnels:get	√	√
Creating a custom authoriz er	POST /v2/{project_id}/ apigw/instances/ {instance_id}/authorizers	apig:autho rizers:crea te	functiongrap h:function:ge tConfig apig:instance s:get	√	√
Deleting a custom authoriz er	DELETE /v2/{project_id}/ apigw/instances/ {instance_id}/authorizers/ {authorizer_id}	apig:autho rizers:dele te	apig:instance s:get	√	√
Querying details of a custom authoriz er	GET /v2/{project_id}/ apigw/instances/ {instance_id}/authorizers/ {authorizer_id}	apig:autho rizers:get	apig:instance s:get	√	√
Querying custom authoriz ers	GET /v2/{project_id}/ apigw/instances/ {instance_id}/authorizers	apig:autho rizers:list	apig:instance s:get	√	√
Updating a custom authoriz er	PUT /V2/{project_id}/apigw/ instances/{instance_id}/ authorizers/ {authorizer_id}	apig:autho rizers:upd ate	apig:instance s:get	√	√
Querying tags	GET /v2/{project_id}/ apigw/instances/ {instance_id}/tags	apig:tags:l ist	apig:instance s:get	√	√
Querying gateway features	GET /v2/{project_id}/ apigw/instances/ {instance_id}/features	apig:featu res:list	apig:instance s:get	√	√
Creating a gateway feature	POST /v2/{project_id}/ apigw/instances/ {instance_id}/features	apig:featu res:create	apig:instance s:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Viewing monitoring data	GET /v2/{project_id}/apigw/instances/{instance_id}/metric-data	apig:metricData:get	apig:instances:get	√	√
Creating a gateway response	POST /V2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses	apig:gatewayResponses:create	apig:instances:get apig:groups:get	√	√
Querying details of a gateway response	GET /V2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}	apig:gatewayResponses:get	apig:instances:get apig:groups:get	√	√
Updating a gateway response	PUT /V2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}	apig:gatewayResponses:update	apig:instances:get apig:groups:get	√	√
Deleting a gateway response	DELETE /V2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}	apig:gatewayResponses:delete	apig:instances:get apig:groups:get	√	√
Querying a gateway response list	GET /V2/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses	apig:gatewayResponses:list	apig:instances:get apig:groups:get	√	√
Creating an AppCode	POST /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes	apig:appCodes:create	apig:instances:get apig:apps:get	√	√
Querying AppCodes of an app	GET /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes	apig:appCodes:list	apig:instances:get apig:apps:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Querying AppCode details	GET /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes/{app_code_id}	apig:appCodes:get	apig:instances:get apig:apps:get	√	√
Updating AppCodes of an app	PUT /V2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes	apig:appCodes:update	apig:instances:get apig:apps:get	√	√
Deleting an AppCode	DELETE /v2/{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes/{app_code_id}	apig:appCodes:delete	apig:instances:get apig:apps:get	√	√
Creating a plug-in	POST /v2/{project_id}/apigw/instances/{instance_id}/plugins	apig:plugins:create	apig:instances:get	√	√
Updating a plugin	PUT /V2/{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}	apig:plugins:update	apig:instances:get	√	√
Querying the plug-ins	GET /v2/{project_id}/apigw/instances/{instance_id}/plugins	apig:plugins:list	apig:instances:get	√	√
Querying APIs bound with a plug-in	GET /v2/{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attached-apis	apig:plugins:listBoundApis	apig:instances:get apig:plugins:get	√	√
Querying plug-ins	GET /v2/{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}	apig:plugins:get	apig:instances:get	√	√
Querying APIs not bound with a plug-in	GET /v2/{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attachable-apis	apig:plugins:listUnboundApis	apig:instances:get apig:plugins:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Deleting a plug-in	DELETE /v2/{project_id}/ apigw/instances/ {instance_id}/plugins/ {plugin_id}	apig:plugi ns:delete	apig:instance s:get	√	√
Querying SSL certificat es	GET /v2/{project_id}/ apigw/certificates	apig:certifi cate:list	-	√	√
Adding an SSL certificat e	POST /v2/{project_id}/ apigw/certificates	apig:certifi cate:creat e	apig:instance s:get	√	Support ed only when the para meter insta nce_i d is carrie d in the reque st.
Deleting an SSL certificat e	DELETE /v2/{project_id}/ apigw/certificates/ {certificate_id}	apig:certifi cate:delet e	-	√	x
Querying details about an SSL certificat e	GET /v2/{project_id}/ apigw/certificates/ {certificate_id}	apig:certifi cate:get	-	√	x

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Modifying an SSL certificate	PUT /v2/{project_id}/apigw/certificates/{certificate_id}	apig:certificate:update	apig:instances:get	√	Supported only when the parameter instance_id is carried in the request.
Querying domain names of an SSL certificate	GET /v2/{project_id}/apigw/certificates/{certificate_id}/attached-domains	apig:certificate:listBoundDomain	-	√	x
Binding an SSL certificate to a domain name	POST /v2/{project_id}/apigw/certificates/{certificate_id}/domains/attach	apig:certificate:batchBindDomain	apig:certificate:get apig:groups:get	√	x
Unbinding an SSL certificate from a domain name	POST /v2/{project_id}/apigw/certificates/{certificate_id}/domains/detach	apig:certificate:batchUnbindDomain	apig:certificate:get apig:groups:get	√	x
Querying VPC endpoint connections	GET /v2/{project_id}/apigw/instances/{instance_id}/vpc-endpoint/connections	apig:instance:listVpcEndpoint	apig:instances:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Acceptin g or rejecting a VPC endpoint connecti on	POST /v2/{project_id}/ apigw/instances/ {instance_id}/vpc- endpoint/connections/ action	apig:insta nce:accept OrRejectV pcEndpoi ntConnecti on	apig:instance s:get	√	√
Querying the whitelist records of a gateway' s VPC endpoint service	GET /v2/{project_id}/ apigw/instances/ {instance_id}/vpc- endpoint/permissions	apig:insta nce:listVpc EndpointP ermission	apig:instance s:get	√	√
Adding whitelist records for a VPC endpoint service	POST/v2/{project_id}/ apigw/instances/ {instance_id}/vpc- endpoint/permissions/ batch-add	apig:insta nce:batch AddVpcEn dpointPer mission	apig:instance s:get	√	√
Deleting whitelist records of a VPC endpoint service	POST/v2/{project_id}/ apigw/instances/ {instance_id}/vpc- endpoint/permissions/ batch-delete	apig:insta nce:batch DeleteVpc EndpointP ermission	apig:instance s:get	√	√
Creating a paramet er orchestra tion rule	POST /v2/{project_id}/ apigw/instances/ {instance_id}/ orchestration	apig:orche stration:cr eate	apig:instance s:get	√	√
Querying orchestra tion rules	GET /v2/{project_id}/ apigw/instances/ {instance_id}/ orchestration	apig:orche stration:lis t	apig:instance s:get	√	√

Permissi on	API	Action	Dependenci es	IAM Proj ect	Enter prise Proje ct
Querying rule details	GET /v2/{project_id}/apigw/instances/{instance_id}/orchestrations/{orchestration_id}	apig:orchestration:get	apig:instances:get	√	√
Updating an orchestration rule	PUT /v2/{project_id}/apigw/instances/{instance_id}/orchestrations/{orchestration_id}	apig:orchestration:update	apig:instances:get	√	√
Deleting an orchestration rule	DELETE /v2/{project_id}/apigw/instances/{instance_id}/orchestrations/{orchestration_id}	apig:orchestration:delete	apig:instances:get	√	√
Querying APIs to which an orchestration rule is bound	GET /v2/{project_id}/apigw/instances/{instance_id}/orchestrations/{orchestration_id}/attached-apis	apig:orchestration:listBoundApis	apig:instances:get	√	√

7 Appendix

7.1 Pagination Query

APIG supports pagination query of resource lists, such as an API list.

To perform a pagination query, add the following parameters to the URL:

- **page_size**: number of records to be displayed on each page. If this parameter is not specified, the default value **20** is used. The maximum value is **500**.
- **page_no**: page number for displaying query results.

Example:

```
GET /v1.0/apigw/apis?page_size=10&page_no=5
```

7.2 Result Filtering

APIG filters query results by object attribute when you query a resource list, such as an API list.

Example:

```
GET /v1.0/apigw/apis?id=xxxx
```

7.3 HTTP Status Codes

[Table 7-1](#) describes common status codes.

Table 7-1 HTTP status codes

Status Code & Message	Description
200 OK	The request has been processed successfully.
204 No Content	The server successfully processed the request and is not returning any content.

Status Code & Message	Description
400 Bad Request	The server failed to process the request. Possible causes include: 1. Malformed request syntax 2. Invalid request message framing
401 Unauthorized	The request requires user authentication. For example, the username and password are required.
403 Forbidden	The server understood the request, but is refusing to fulfill it.
404 Not Found	The server has not found anything matching the request URI.
405 Method Not Allowed	The method specified in the request line is not allowed for the resource identified by the request URI.
406 Not Acceptable	The response generated by the server could not be accepted by the client.
407 Proxy Authentication Required	You must first authenticate yourself with the proxy.
408 Request Timeout	The server timed out waiting for the request.
409 Conflict	The request could not be completed due to a conflict with the current state of the resource.
410 Gone	The requested resource is no longer available at the server and no forwarding address is known.
412 Precondition Failed	The server does not meet one of the preconditions that the requester put on the request.
500 Internal Server Error	The server encountered an unexpected condition which prevented it from fulfilling the request.
501 Not Implemented	The server does not support the functionality required to fulfill the request.
502 Bad Gateway	The server, while acting as a gateway or proxy, received an invalid response from the upstream server it accessed in attempting to fulfill the request.
503 Service Unavailable	The request could not be processed by the server because the server is being maintained or overloaded.
504 Gateway Timeout	The server was acting as a gateway or proxy and did not receive a timely response from the upstream server.

7.4 Error Codes

If an error code starting with APIGW is returned after you call an API, rectify the fault by referring to the instructions provided in [API Gateway Error Codes](#).

Status Code	Error Codes	Error Message	Description	Solution
204	APIG.0000	Successful	Successful	You do not need to take any actions.
400	APIC.7211	Parameter value does not match the rules	Parameter value does not match the rules	Modify the parameter value.
400	APIC.7230	The maintenance time window must be 4 hours.	The maintenance time window must be 4 hours.	Modify the maintenance time window to 4 hours.
400	APIC.7235	The maintenance time window must start or end with 2, 6, 10, 14, 18, or 22.	The maintenance time window must start or end with 2, 6, 10, 14, 18, or 22.	Modify the maintenance time window to start or end with 2, 6, 10, 14, 18, or 22.
400	APIC.7238	An AZ must be specified.	An AZ must be specified.	Specify an AZ when creating a gateway.
400	APIC.7239	Invalid IP address.	Invalid IP address.	Enter a valid IP address.
400	APIC.7241	An enterprise project ID must be specified if you are an enterprise user.	An enterprise project ID must be specified if you are an enterprise user.	Specify an enterprise project ID.
400	APIC.7242	Load balancing is not supported by this edition.	Load balancing is not supported by this edition.	Change the gateway edition.

Status Code	Error Codes	Error Message	Description	Solution
400	APIC.7243	Scale-up is not supported by this edition.	Scale-up is not supported by this edition.	Change the gateway edition.
400	APIC.7244	The bandwidth cannot be updated.	The bandwidth cannot be updated.	Do not perform this operation.
400	APIC.7254	IPv6 access not supported.	IPv6 access not supported.	Contact technical support.
400	APIC.7255	IPv6 not supported for the subnet used when creating the gateway or enabling IPv6 access.	IPv6 not supported for the subnet used when creating the gateway or enabling IPv6 access.	Use another subnet that supports IPv6.
400	APIC.7257	The custom inbound port is bound to a custom domain name.	The port is bound to another API group.	Delete or modify the domain name bound to the custom inbound port.
400	APIC.7258	Port already defined.	Port already defined.	Enter another port number.
400	APIC.7312	The AZ does not support IPv6.	The AZ does not support IPv6.	Use an AZ that supports IPv6.
400	APIC.7313	The bandwidth for IPv6 cannot be less than 5 MB.	The bandwidth for IPv6 cannot be less than 5 MB.	Increase the bandwidth
400	APIC.7500	The gateway name already exists.	The gateway name already exists.	Use another gateway name.
400	APIC.7503	Parameters az and azList cannot be used at the same time.	Parameters az and azList cannot be used at the same time.	Delete az or azList.

Status Code	Error Codes	Error Message	Description	Solution
400	APIC.7505	The gateway ID already exists.	The gateway ID already exists.	Change the gateway ID.
400	APIC.9206	Failed to create the gateway.	Failed to create the gateway.	If the resources are insufficient, expand the resources. If the network is abnormal, check the service network for connectivity.
400	APIC.9208	Failed to disable public outbound access.	Failed to disable public outbound access.	Contact technical support to view the logs.
400	APIC.9210	create cloud nat eip failed	create cloud nat eip failed	Contact technical support to view the background logs.
400	APIC.9211	update bandwidth size failed	update bandwidth size failed	Contact technical support.
400	APIC.9215	Failed to scale up the gateway.	Failed to scale up the gateway.	Contact technical support to view the background logs.
400	APIC.9216	Failed to enable public inbound access.	Failed to enable public inbound access.	Contact technical support to view the background logs.
400	APIC.9217	Failed to accept VPC peering connection or create route	Failed to accept VPC peering connection or create route	Connect technical support to view background logs.
400	APIC.9218	Create instance failed due to insufficient quota.	Create instance failed due to insufficient quota.	Increase the quota and try again.

Status Code	Error Codes	Error Message	Description	Solution
400	APIC.9219	Create instance failed due to insufficient resources.	Create instance failed due to insufficient resources.	Expand the resource capacity and try again.
400	APIC.9222	Lock gateway operation failed.	Lock gateway operation failed.	Contact technical support.
400	APIC.9223	Delete custom inbound port failed.	Delete custom inbound port failed.	Try again later or contact technical support.
400	APIC.9224	Add custom inbound port failed.	Add custom inbound port failed.	Try again later or contact technical support.
400	APIG.1119	No permissions to perform this operation.	No permissions to perform this operation.	Apply for the required permissions and try again.
400	APIG.1120	No permissions to create ELB channels.	No permissions to create ELB channels.	Ensure that the ELB channel belongs to your account. If you are an IAM user, apply for the required permissions.
400	APIG.1201	The resources belong to different tenants.	The resources belong to different tenants.	Ensure that the resources belong to the same tenant.
400	APIG.2000	Parameter error.	Parameter error.	Modify the request parameters based on the reasons stated in the API response.
400	APIG.2001	The request parameters must be specified.	The request parameters must be specified.	Set request parameters.

Status Code	Error Codes	Error Message	Description	Solution
400	APIG.2002	The parameter value is too small.	The parameter value is too small.	Modify the request parameter.
400	APIG.2003	The parameter value is too large.	The parameter value is too large.	Modify the request parameter.
400	APIG.2004	The parameter value is outside the allowable range.	The parameter value is outside the allowable range.	Modify the request parameter.
400	APIG.2005	The parameter is too short.	The parameter is too short.	Modify the request parameter.
400	APIG.2006	The parameter is too long.	The parameter is too long.	Modify the request parameter.
400	APIG.2007	Invalid length.	Invalid length.	Modify the request parameter.
400	APIG.2008	Only letters are allowed.	Only letters are allowed.	Modify the request parameter.
400	APIG.2009	Only digits are allowed.	Only digits are allowed.	Modify the request parameter.
400	APIG.2010	Only letters and digits are allowed.	Only letters and digits are allowed.	Modify the request parameter.
400	APIG.2011	Invalid parameter value.	Invalid parameter value.	Modify the request parameter.
400	APIG.2012	Invalid parameter value.	Invalid parameter value.	Modify the request parameter.

Status Code	Error Codes	Error Message	Description	Solution
400	APIG.2013	Only letters, digits, hyphens (-), and underscores (_) are allowed.	Only letters, digits, hyphens (-), and underscores (_) are allowed.	Modify the request parameter.
400	APIG.2014	Invalid email address.	Invalid email address.	Modify the request parameter.
400	APIG.2015	Invalid IP address.	Invalid IP address.	Modify the request parameter.
400	APIG.2016	The characters are not encoded using Base 64.	The characters are not encoded using Base 64.	Change the value of the request parameter to a Base 64-encoded character string.
400	APIG.2017	Invalid mobile number.	Invalid mobile number.	Modify the request parameter.
400	APIG.2018	Invalid telephone number.	Invalid telephone number.	Modify the request parameter.
400	APIG.2019	Invalid telephone or mobile number.	Invalid telephone or mobile number.	Modify the request parameter.
400	APIG.2020	Invalid postal code.	Invalid postal code.	Modify the request parameter.
400	APIG.2021	The URL domain is not included in the IP address whitelist.	The URL domain is not included in the IP address whitelist.	Modify the request parameter.
400	APIG.2022	The URL domain is included in the IP address blacklist.	The URL domain is included in the IP address blacklist.	Modify the request parameter.

Status Code	Error Codes	Error Message	Description	Solution
400	APIG.2023	URL domain CNAME resolution failed.	URL domain CNAME resolution failed.	Register the CNAME resolution record of the domain name.
400	APIG.2024	Invalid URL domain.	Invalid URL domain.	Use a correct domain name.
400	APIG.2025	Invalid port number.	Invalid port number.	Use a correct port number.
400	APIG.2026	The request path parameters are not defined.	The request path parameters are not defined.	Add the parameters contained in the request path to the request parameters.
400	APIG.2027	The backend path parameters are not defined.	The backend path parameters are not defined.	Add the parameters contained in the backend request path to the backend parameters.
400	APIG.2028	The request parameters mapped to the backend parameters are not defined.	The request parameters mapped to the backend parameters are not defined.	Map the backend parameters to the correct request parameters.
400	APIG.2029	The default certificate already exists.	The default certificate already exists.	Contact technical support.
400	APIG.2030	Bad request for debugging the API.	Bad request for debugging the API.	Set correct API debugging parameters.
400	APIG.2034	The domain name has not been filed. File it first.	The domain name has not been filed. File it first.	Complete ICP filing for the domain name.
400	APIG.2035	The ICP Filing System is busy. Please try again later.	The ICP Filing System is busy. Please try again later.	Contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
400	APIG.2036	Only APIs that use custom authentication can have authorizer parameters.	Only APIs that use custom authentication can have authorizer parameters.	Delete unnecessary parameters.
400	APIG.2041	Invalid microservice.	Invalid microservice.	Change service_id to a valid microservice ID.
400	APIG.2042	Invalid engine.	Invalid engine.	Change engine_id to a valid microservice engine ID.
400	APIG.2044	Invalid title of info	Invalid Info.title	The Info.title must meet the documents
400	APIG.2045	Parse Servers error. The Servers must meet the documents	Servers field parsing error. Servers field is invalid	The Servers must meet the documents
400	APIG.2046	Incorrect custom authentication timeout.	Incorrect custom authentication timeout.	Modify the custom authentication timeout. It should be less than or equal to the function execution timeout and the V2 API timeout (600s).
400	APIG.2047	Incorrect number of retries for custom authentication.	Set the number of custom authentication retries to a value between 0 and 10.	Set the number of custom authentication retries to a value between 0 and 10.
400	APIG.2048	Incorrect Nacos configurations	Incorrect Nacos configurations	Correct the Nacos configurations.

Status Code	Error Codes	Error Message	Description	Solution
400	APIG.2049	The port is not in the defined custom inbound ports.	The port is not in the defined custom inbound ports.	Use the default HTTP/HTTPS port, or define a new port in the inbound rule.
400	APIG.2050	The combination of this domain name and port already exists.	The combination of this domain name and port already exists.	Specify another domain name or port number.
400	APIG.2051	A domain name cannot be bound with different certificates.	A domain name cannot be bound with different certificates.	Bind the same certificate.
400	APIG.2101	The certificate and private key do not match.	The certificate and private key do not match.	Use a certificate and private key that match each other.
400	APIG.2102	The certificate has expired.	The certificate has expired.	Use a valid certificate.
400	APIG.2103	The certificate domain name and the custom domain name do not match.	The certificate domain name and the custom domain name do not match.	Ensure that the domain name in the certificate is the same as the custom domain name.
400	APIG.2104	The certificate chain is not matched.	The certificate chain is not matched.	In a certificate chain, ensure that the server certificate is in the first place and followed by other certificates in sequence.
400	APIG.2105	Encrypted private keys are not supported.	Encrypted private keys are not supported.	Use unencrypted private keys.
400	APIG.2106	Invalid certificate or private key.	Invalid certificate or private key.	Use a correct certificate and private key.

Status Code	Error Codes	Error Message	Description	Solution
400	APIG.2108	Microservice unavailable.	Microservice unavailable.	Change service_id to the ID of an available microservice.
400	APIG.2109	Invalid certificate. SAN missing.	Invalid certificate. SAN missing.	Generate a new certificate that contains a SAN.
400	APIG.3073	The IP address or IP address/CIDR mask does not exist.	The IP address or IP address/CIDR mask does not exist.	Check the IP address or IP address/CIDR mask.
400	APIG.3148	Invalid certificate. Add one that expires before January 19, 2038 03:14:07 UTC.	Invalid certificate. Add one that expires before January 19, 2038 03:14:07 UTC.	Invalid certificate. Add one that expires before January 19, 2038 03:14:07 UTC.
400	APIG.3153	The number of custom GeolPs exceeds the limit.	The number of custom GeolPs exceeds the limit.	Delete unnecessary custom GeolPs.
400	APIG.3201	The API group name already exists.	The API group name already exists.	Use another name.
400	APIG.3202	The API name already exists.	The API name already exists.	Use another name.
400	APIG.3203	The app name already exists.	The app name already exists.	Use another name.
400	APIG.3204	The request throttling policy name already exists.	The request throttling policy name already exists.	Use another name.
400	APIG.3205	The environment name already exists.	The environment name already exists.	Use another name.

Status Code	Error Codes	Error Message	Description	Solution
400	APIG.3206	The access control policy name already exists.	The access control policy name already exists.	Use another name.
400	APIG.3207	The signature key name already exists.	The signature key name already exists.	Use another name.
400	APIG.3208	The VPC channel name already exists.	The VPC channel name already exists.	Use another name.
400	APIG.3209	The parameter name already exists.	The parameter name already exists.	Use another name.
400	APIG.3210	The backend policy name already exists.	The backend policy name already exists.	Use another name.
400	APIG.3211	The authorizer name already exists.	The authorizer name already exists.	Use another name.
400	APIG.3212	The identity source name already exists.	The identity source name already exists.	Use another name.
400	APIG.3213	The tag name already exists.	The tag name already exists.	Use another name.
400	APIG.3216	The response name already exists.	The response name already exists.	Use another name.
400	APIG.3301	The API already exists.	The API already exists.	Change the request method and URL of the API.
400	APIG.3302	The excluded configuration already exists.	The excluded configuration already exists.	Use another name.
400	APIG.3303	The environment variable already exists.	The environment variable already exists.	Use another name.

Status Code	Error Codes	Error Message	Description	Solution
400	APIG.3304	The purchasing order already exists.	The purchasing order already exists.	Contact technical support.
400	APIG.3305	The URL domain name already exists.	The URL domain name already exists.	Contact technical support.
400	APIG.3306	The IP address already exists.	The IP address already exists.	Contact technical support.
400	APIG.3308	The excluded request throttling configuration already exists.	The excluded request throttling configuration already exists.	Contact technical support.
400	APIG.3309	The operation has already been performed.	The operation has already been performed.	Contact technical support.
400	APIG.3310	The AppKey already exists.	The AppKey already exists.	Use another AppKey.
400	APIG.3316	The API authorization record already exists.	The API authorization record already exists.	Use another API or app.
400	APIG.3330	VPC already bound to a microservice.	VPC already bound to a microservice.	Change vpc_channel_id to another ID not bound to any microservice.
400	APIG.3331	The orchestration rule name already exists.	The orchestration rule name already exists.	Use a unique rule name.
400	APIG.3332	The IP address or IP address/CIDR mask already exists.	The IP address or IP address/CIDR mask already exists.	Check whether the IP address or IP address/CIDR mask is unique.

Status Code	Error Codes	Error Message	Description	Solution
400	APIG.3600	JSON or YAML format error.	JSON or YAML format error.	Check whether the file to be imported is in correct YAML or JSON format.
400	APIG.3601	The Swagger file version must be 2.0.	The Swagger file version must be 2.0.	Ensure that the Swagger file version is 2.0.
400	APIG.3602	Syntax error in the Swagger file.	Syntax error in the Swagger file.	Check for syntax errors in the Swagger file.
400	APIG.3603	The Swagger file content is too long.	The Swagger file content is too long.	Reduce the size of the Swagger file.
400	APIG.3608	The API Designer does not support API modification.	The API Designer does not support API modification.	Contact technical support.
400	APIG.3609	The input file is empty.	The input file is empty.	Use a file that is not empty.
400	APIG.3710	The VPC channel is being used by another third_auth plugin	The VPC channel is being used by another third_auth plugin	Unbind the third-party plug-in from the load balance channel, and then delete the load balance channel.
400	APIG.3715	A domain name can only be bound with CA certificates of the same algorithm type.	A domain name can only be bound with CA certificates of the same algorithm type.	Unbind the existing CA certificates and try again.
400	APIG.3717	Two-way TLS authentication not supported for HTTP or GRPC backend requests.	Two-way TLS authentication not supported for HTTP or GRPC backend requests.	Disable two-way TLS authentication first.

Status Code	Error Codes	Error Message	Description	Solution
401	APIC.7100	Token missing. Log in again or try again later.	Token missing. Log in again or try again later.	Provide a token.
401	APIC.7101	Token expired. Try again later.	Token expired. Try again later.	Obtain a new token.
401	APIC.7102	Incorrect token or token resolution failure	Incorrect token or token resolution failure	Contact technical support to check the token encryption/decryption setting.
401	APIC.7103	Token contains no project information.	Token contains no project information.	Specify project information when obtaining a token.
401	APIC.7105	Token contains no user information.	Token contains no user information.	Specify user information when obtaining a token.
401	APIC.7107	Token contains no role information.	Token contains no role information.	Specify role information when obtaining a token.
401	APIG.1000	Token missing. Log in again or try again later.	Token missing. Log in again or try again later.	Provide a token.
401	APIG.1001	Session expired. Please try again later.	Session expired. Please try again later.	Obtain another token and try again.
401	APIG.1002	Incorrect token or token resolution failed.	Incorrect token or token resolution failed.	Use a correct token.
401	APIG.1003	Token contains no project information.	Token contains no project information.	Use a token containing project information.

Status Code	Error Codes	Error Message	Description	Solution
401	APIG.1005	No permissions to request this method	No permissions to request this method	Use a token with the required permissions.
401	APIG.1007	Token contains no domain information.	Token contains no domain information.	Contact technical support.
401	APIG.1008	Invalid domain.	Invalid domain.	Contact technical support.
401	APIG.1009	Token contains no user information.	Token contains no user information.	Use a token containing user information.
401	APIG.1010	PDP server connection failed.	PDP server connection failed.	Contact technical support.
401	APIG.1011	You can request resources only after you complete real-name authentication.	You can request resources only after you complete real-name authentication.	Perform real-name authentication for your account and try again.
401	APIG.1012	Your account balance is insufficient. Top up your account.	Your account balance is insufficient. Top up your account.	Top up your account.
401	APIG.1013	Your account has been frozen. Some functions become unavailable. To unfreeze your account, contact customer service.	Your account has been frozen. Some functions become unavailable. To unfreeze your account, contact customer service.	Restore your account and try again.

Status Code	Error Codes	Error Message	Description	Solution
403	APIC.7106	Operation restricted. Check at My Account.	Operation restricted. Check at My Account.	Use a token with the required permissions.
403	APIC.7108	Access denied because your account is frozen.	Access denied because your account is frozen.	Unfreeze your account first.
403	APIC.7109	Access denied because your account is suspended.	Access denied because your account is suspended.	Restore your account first.
403	APIC.7110	Your account only has read permissions and can only send GET requests.	Your account only has read permissions and can only send GET requests.	Contact the account administrator to grant you administrator or fine-grained permissions.
403	APIC.7111	The requested resource does not belong to your account.	The requested resource does not belong to your account.	Use a correct token.
403	APIC.7118	User domain does not match.	User domain does not match.	Check the domain info.
403	APIC.7130	No permissions to access gateways in other projects.	No permissions to access gateways in other projects.	Specify the correct project ID.
403	APIC.7134	No permissions to access this enterprise project.	No permissions to access this enterprise project.	Use an enterprise project that you have permissions to access.
403	APIC.7300	You do not have permission to perform action {x} on resource {x}.	You do not have permission to perform action {x} on resource {x}.	Check your permissions.

Status Code	Error Codes	Error Message	Description	Solution
403	APIC.7400	Maximum number of gateways reached.	Maximum number of gateways reached.	Contact technical support to increase the gateway quota.
403	APIC.7402	The number of tags exceeds the maximum allowed limit.	The number of tags exceeds the maximum allowed limit.	Delete unnecessary tags.
403	APIC.7403	The number of custom inbound ports has reached the maximum.	The number of custom inbound ports has reached the maximum.	Increase the quota for custom inbound ports.
403	APIG.1020	Insufficient permissions.	Insufficient permissions.	Grant the read and write permissions to the user.
403	APIG.1101	No permissions to perform operations on this API group.	No permissions to perform operations on this API group.	Ensure that the API group belongs to your account. If you are an IAM user, apply for the required permissions.
403	APIG.1102	No permissions to perform operations on this API.	No permissions to perform operations on this API.	Ensure that the API belongs to your account. If you are an IAM user, apply for the required permissions.
403	APIG.1103	No permissions to perform operations on this environment.	No permissions to perform operations on this environment.	Ensure that the environment belongs to your account. If you are an IAM user, apply for the required permissions.

Status Code	Error Codes	Error Message	Description	Solution
403	APIG.1104	No permissions to perform operations on this app.	No permissions to perform operations on this app.	Ensure that the app belongs to your account. If you are an IAM user, apply for the required permissions.
403	APIG.1105	No permissions to perform operations on this request throttling policy.	No permissions to perform operations on this request throttling policy.	Ensure that the request throttling policy belongs to your account. If you are an IAM user, apply for the required permissions.
403	APIG.1106	No permissions to perform operations on this access control policy.	No permissions to perform operations on this access control policy.	Ensure that the access control policy belongs to your account. If you are an IAM user, apply for the required permissions.
403	APIG.1107	No permissions to perform operations on this configuration.	No permissions to perform operations on this configuration.	Contact technical support.
403	APIG.1108	No permissions to perform operations on this excluded configuration.	No permissions to perform operations on this excluded configuration.	Contact technical support.
403	APIG.1109	No permissions to perform operations on this app authorization record.	No permissions to perform operations on this app authorization record.	Ensure that the app authorization information belongs to your account. If you are an IAM user, apply for the required permissions.

Status Code	Error Codes	Error Message	Description	Solution
403	APIG.1110	No permissions to perform operations on this environment variable.	No permissions to perform operations on this environment variable.	Ensure that the environment variable belongs to your account. If you are an IAM user, apply for the required permissions.
403	APIG.1111	No permissions to perform operations on this subscription record.	No permissions to perform operations on this subscription record.	Ensure that the subscription belongs to your account. If you are an IAM user, apply for the required permissions.
403	APIG.1112	No permissions to perform operations on this signature key.	No permissions to perform operations on this signature key.	Ensure that the signature key belongs to your account. If you are an IAM user, apply for the required permissions.
403	APIG.1113	No permissions to perform operations on this VPC channel.	No permissions to perform operations on this VPC channel.	Ensure that the VPC channel belongs to your account. If you are an IAM user, apply for the required permissions.
403	APIG.1115	No permissions to perform operations on this certificate.	No permissions to perform operations on this certificate.	Ensure that the certificate belongs to your account. If you are an IAM user, apply for the required permissions.
403	APIG.1116	No permissions to perform operations on this on-sale API.	No permissions to perform operations on this on-sale API.	Ensure that the API belongs to your account. If you are an IAM user, apply for the required permissions.

Status Code	Error Codes	Error Message	Description	Solution
403	APIG.1136	No permissions to perform operations on this instance.	No permissions to perform operations on this instance.	Contact technical support.
403	APIG.1137	No permissions to perform operations on this authorizer.	No permissions to perform operations on this authorizer.	Ensure that the custom authorizer belongs to your account. If you are an IAM user, apply for the required permissions.
403	APIG.1140	No permissions to perform operations on this feature.	No permissions to perform operations on this feature.	Ensure that the feature belongs to your account. If you are an IAM user, apply for the required permissions.
403	APIG.1200	No permissions to perform operations on this API Swagger file.	No permissions to perform operations on this API Swagger file.	Ensure that the Swagger file belongs to your account. If you are an IAM user, apply for the required permissions.
403	APIG.1301	No permissions to perform operations on this domain	No permissions to perform operations on this domain	The domain to be operated must be under your own account.
403	APIG.3100	The number of resources exceeds the maximum allowed limit.	The number of resources exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3101	The number of API groups exceeds the maximum allowed limit.	The number of API groups exceeds the maximum allowed limit.	Contact technical support to increase the quota.

Status Code	Error Codes	Error Message	Description	Solution
403	APIG.3102	The number of APIs exceeds the maximum allowed limit.	The number of APIs exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3103	The number of apps exceeds the maximum allowed limit.	The number of apps exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3104	The number of environments exceeds the maximum allowed limit.	The number of environments exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3105	The number of signature keys exceeds the maximum allowed limit.	The number of signature keys exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3106	The number of variables exceeds the maximum allowed limit.	The number of variables exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3107	The number of request throttling policies exceeds the maximum allowed limit.	The number of request throttling policies exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3108	The number of domain names exceeds the maximum allowed limit.	The number of domain names exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3109	The number of VPC channels exceeds the maximum allowed limit.	The number of VPC channels exceeds the maximum allowed limit.	Contact technical support to increase the quota.

Status Code	Error Codes	Error Message	Description	Solution
403	APIG.3110	The number of cloud servers in the VPC channel exceeds the maximum allowed limit.	The number of cloud servers in the VPC channel exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3111	The number of parameters in req_params exceeds the maximum allowed limit.	The number of parameters in req_params exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3112	The number of access control policies exceeds the maximum allowed limit.	The number of access control policies exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3113	The number of API backend policies exceeds the maximum allowed limit.	The number of API backend policies exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3114	The number of policy conditions exceeds the maximum allowed limit.	The number of policy conditions exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3116	The number of authorizers exceeds the maximum allowed limit.	The number of authorizers exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3117	The number of identity sources exceeds the maximum allowed limit.	The number of identity sources exceeds the maximum allowed limit.	Contact technical support to increase the quota.

Status Code	Error Codes	Error Message	Description	Solution
403	APIG.3125	The number of APIs in the API group exceeds the maximum allowed limit.	The number of APIs in the API group exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3127	The number of APIs has reached the upper limit. A maximum of xxx APIs can be imported at a time.	The number of APIs has reached the upper limit. A maximum of xxx APIs can be imported at a time.	Reduce the number of APIs to import.
403	APIG.3131	The number of AppCodes exceeds the maximum allowed limit.	The number of AppCodes exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3132	The number of Swagger APIs in the API group exceeds the maximum allowed limit.	The number of Swagger APIs in the API group exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3133	The number of API tags exceeds the maximum allowed limit.	The number of API tags exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3136	The number of responses exceeds the maximum allowed limit.	The number of responses exceeds the maximum allowed limit.	Contact technical support to increase the quota.
403	APIG.3150	The number of orchestration rules exceeds the maximum.	The number of orchestration rules exceeds the maximum.	Contact technical support to increase the quota of orchestration rules.

Status Code	Error Codes	Error Message	Description	Solution
403	APIG.3151	The number of orchestration rules bound to the API exceeds the maximum.	The number of orchestration rules bound to the API exceeds the maximum.	Contact technical support to increase the quota of orchestration rules that can be bound to the API.
403	APIG.3411	The APIs belong to different tenants.	The APIs belong to different tenants.	This operation is not allowed.
403	APIG.3412	The API provider has been frozen.	The API provider has been frozen.	Contact technical support.
403	APIG.3414	The VPC channel is already being used by another API.	The VPC channel is already being used by another API.	Delete the API associated with the VPC channel and then delete the VPC channel.
403	APIG.3415	The API group cannot be deleted because it contains APIs.	The API group cannot be deleted because it contains APIs.	Delete the APIs in the API group and then delete the API group.
403	APIG.3416	The API cannot be deleted because it has been published.	The API cannot be deleted because it has been published.	Take the API offline and then delete it.
403	APIG.3418	The environment contains published APIs.	The environment contains published APIs.	This operation is not allowed.
403	APIG.3420	The API group is no longer available on the marketplace.	The API group is no longer available on the marketplace.	Check whether the API group has been listed on the marketplace.

Status Code	Error Codes	Error Message	Description	Solution
403	APIG.3447	The access control policy cannot be deleted because it has been bound to APIs.	The access control policy cannot be deleted because it has been bound to APIs.	Delete the APIs bound with the access control policy and then delete the access control policy.
403	APIG.3451	The request throttling policy cannot be deleted because it has been bound to APIs.	The request throttling policy cannot be deleted because it has been bound to APIs.	Delete the APIs bound with the request throttling policy and then delete the request throttling policy.
403	APIG.3471	The operation cannot be performed on this type of VPC channel.	The operation cannot be performed on this type of VPC channel.	This operation is not allowed.
403	APIG.3472	The load balancer is already being used by another VPC channel.	The load balancer is already being used by another VPC channel.	Unbind the load balancer from the VPC channel.
403	APIG.3473	The load balancer has already been bound to another endpoint service.	The load balancer has already been bound to another endpoint service.	This operation is not allowed.
403	APIG.3474	The API group ID in the URL does not match the API group to which the URL domain has been bound.	The API group ID in the URL does not match the API group to which the URL domain has been bound.	Change the API group specified in the URL to the API group associated with the domain name.
404	APIC.7301	Instance spec not found	Instance spec not found	Use a valid instance spec.

Status Code	Error Codes	Error Message	Description	Solution
404	APIC.7302	Instance not found	Instance not found	Check whether the instance exists, and use a valid instance ID.
404	APIC.7307	The security group does not exist in the VPC.	The security group does not exist in the VPC.	Use an existing security group.
404	APIC.7310	The region does not have any AZs.	The region does not have any AZs.	Use another region.
404	APIC.7311	The NAT EIP does not exist in the VPC.	The NAT EIP does not exist in the VPC.	Use an existing NAT EIP.
404	APIC.7314	The VPC Endpoint of the gateway does not exist.	The VPC Endpoint of the gateway does not exist.	Contact technical support to check the VPC Endpoint.
404	APIG.3001	The API group does not exist	The API group does not exist	Check whether the API group exists.
404	APIG.3002	The API does not exist.	The API does not exist.	Check whether the API exists.
404	APIG.3003	The environment does not exist.	The environment does not exist.	Check whether the environment exists.
404	APIG.3004	The app does not exist.	The app does not exist.	Check whether the app exists.
404	APIG.3005	The request throttling policy does not exist.	The request throttling policy does not exist.	Check whether the request throttling policy exists.
404	APIG.3006	The access control policy does not exist.	The access control policy does not exist.	Check whether the access control policy exists.
404	APIG.3007	The configuration does not exist.	The configuration does not exist.	Check whether the configuration exists.

Status Code	Error Codes	Error Message	Description	Solution
404	APIG.3008	The excluded configuration does not exist.	The excluded configuration does not exist.	Check whether the excluded configuration exists.
404	APIG.3009	The app authorization record does not exist.	The app authorization record does not exist.	Check whether the app authorization record exists.
404	APIG.3010	The access control policy binding record does not exist.	The access control policy binding record does not exist.	Check whether the access control policy binding record exists.
404	APIG.3011	The environment variable does not exist.	The environment variable does not exist.	Check whether the environment variable exists.
404	APIG.3012	The request throttling policy binding record does not exist.	The request throttling policy binding record does not exist.	Check whether the request throttling policy binding record exists.
404	APIG.3013	The excluded request throttling configuration does not exist.	The excluded request throttling configuration does not exist.	Check whether the excluded request throttling configuration exists.
404	APIG.3014	The pre-subscription record does not exist.	The pre-subscription record does not exist.	Check whether the purchasing record exists.
404	APIG.3015	The API publication record does not exist.	The API publication record does not exist.	Check whether the API publication record exists.
404	APIG.3016	The API group listing information does not exist.	The API group listing information does not exist.	Check whether the API group has been listed on the marketplace.

Status Code	Error Codes	Error Message	Description	Solution
404	APIG.3017	The signature key does not exist.	The signature key does not exist.	Check whether the signature key exists.
404	APIG.3018	The signature key binding record does not exist.	The signature key binding record does not exist.	Check whether the signature key binding record exists.
404	APIG.3019	The function URN does not exist.	The function URN does not exist.	Check whether the function URN exists.
404	APIG.3020	The URL domain does not exist.	The URL domain does not exist.	Check whether the domain name exists.
404	APIG.3021	The SSL certificate does not exist.	The SSL certificate does not exist.	Check whether the SSL certificate exists.
404	APIG.3022	The API version does not exist.	The API version does not exist.	Check whether the API version exists.
404	APIG.3023	The VPC channel does not exist.	The VPC channel does not exist.	Check whether the VPC channel exists.
404	APIG.3024	The cloud server does not exist.	The cloud server does not exist.	Check whether the cloud server exists in the VPC channel.
404	APIG.3025	The certificate does not exist.	The certificate does not exist.	Check whether the certificate exists.
404	APIG.3030	The instance does not exist.	The instance does not exist.	Check whether the instance exists.
404	APIG.3072	The specified task does not exist	The specified task does not exist	The specified task does not exist
404	APIG.3081	The authorizer does not exist.	The authorizer does not exist.	Check whether the custom authorizer exists.

Status Code	Error Codes	Error Message	Description	Solution
404	APIG.3082	The AppCode does not exist.	The AppCode does not exist.	Check whether the AppCode exists.
404	APIG.3087	The feature configuration does not exist.	The feature configuration does not exist.	Check whether the feature configuration exists.
404	APIG.3090	The API Swagger file does not exist.	The API Swagger file does not exist.	Check whether the Swagger file exists.
404	APIG.3092	The ECS does not exist.	The ECS does not exist.	The ECS has already been deleted, or the ECS ID is incorrect.
404	APIG.3094	Instance task does not exist.	Instance task does not exist.	Instance task is deleted or task ID is invalid.
404	APIG.3095	The orchestrations does not exist	The orchestrations does not exist	Check whether the orchestration rule corresponding to orchestration_id in the request parameter exists.
404	APIG.3097	The binding record of this SSL certificate and domain name does not exist.	The binding record of this SSL certificate and domain name does not exist.	Check whether the binding record exists.
409	APIC.7701	Instance status conflict.	Instance status conflict.	Try again after the gateway upgrade is complete.
409	APIC.7707	Scaling up to the same specifications is not allowed.	Scaling up to the same specifications is not allowed.	Scale up to other specifications.

Status Code	Error Codes	Error Message	Description	Solution
409	APIC.7709	Public network access is enabled for the gateway.	Public network access is enabled for the gateway.	Disable public network access and try again.
409	APIC.7710	ELB is available only when the instance is in the Available state.	ELB is available only when the instance is in the Available state.	Contact technical support to restore the gateway status to Running, and try again.
409	APIC.7711	Public inbound access is enabled for the instance	Public inbound access is enabled for the instance.	Disable public inbound access and try again.
409	APIC.7712	The gateway operation has already been locked.	The gateway operation has already been locked.	Pay the order.
409	APIG.1149	No permission for this instance task.	No permission for this instance task.	Use a token of the correct project.
409	APIG.3491	The default response cannot be deleted.	The default response cannot be deleted.	This operation is not allowed.
409	APIG.3492	The default response name cannot be modified.	The default response name cannot be modified.	This operation is not allowed.
409	APIG.3707	Only published APIs can be bound with plug-ins.	Only published APIs can be bound with plug-ins.	Publish the API and try again.
409	APIG.3708	The key usage of the certificate does not match	The key usage of the certificate does not match	Use matched key usage

Status Code	Error Codes	Error Message	Description	Solution
409	APIG.3709	The signature algorithm of the certificate does not match	The signature algorithm of the certificate does not match	Change signature algorithm type
409	APIG.3711	A configuration parameter can be modified only once per minute.	A configuration parameter can be modified only once per minute.	Try again after 1 minute.
409	APIG.3712	User domain does not match.	User domain does not match.	Check the domain info.
409	APIG.3716	The orchestration rule is currently in use by another API.	The orchestration rule is currently in use by another API.	Unbind the orchestration rule from the API.
409	APIG.3718	An instance task is currently being processed.	An instance task is currently being processed.	Start a new task after the current one is complete.
409	APIG.3719	The load balance channel is referenced by another load balance channel and cannot be deleted.	The load balance channel is referenced by another load balance channel and cannot be deleted.	Delete the referencing load balance channel first.
412	APIG.3458	The feature is not supported by the current instance.	The feature is not supported by the current instance.	Contact technical support.
412	APIG.3713	orchestration_mapped_param cannot be modified.	orchestration_mapped_param cannot be modified.	Do not modify orchestration_mapped_param.

Status Code	Error Codes	Error Message	Description	Solution
412	APIG.3714	The backend request protocol does not support SM cryptographic algorithms.	The backend request protocol does not support SM cryptographic algorithms.	Change the protocol to HTTPS.
500	APIC.7253	Internal configuration error.	Internal configuration error.	Check the internal configuration.
500	APIC.9000	Failed to request internal service	Failed to request internal service	Contact technical support to view the background logs.
500	APIC.9005	Order creation failed.	Order creation failed.	Contact technical support to view background logs related to CBC.
500	APIC.9007	Failed to access VPCEP	Failed to access VPCEP	Contact technical support to view logs related to VPCEP.
500	APIC.9100	Failed to access the database.	Failed to access the database.	Contact technical support to view background logs related to the database.
500	APIC.9200	Failed to query AZ information.	Failed to query AZ information.	Contact technical support to view the background logs.
500	APIC.9204	Failed to bind the EIP.	Failed to bind the EIP.	Contact technical support to view the background logs.
500	APIC.9209	Failed to access EPS.	Failed to access EPS.	Contact technical support to view logs related to EPS.

Status Code	Error Codes	Error Message	Description	Solution
500	APIC.9999	System error. Contact technical support.	System error. Contact technical support.	Contact technical support to view background logs of the management plane and locate the fault.
500	APIG.1029	PDP5 cannot be connected.	PDP5 cannot be connected.	Check the PDP5 connection.
500	APIG.3500	Failed to synchronize data to etcd.	Failed to synchronize data to etcd.	Contact technical support.
500	APIG.9002	Invalid function URN.	Invalid function URN.	Use a valid function URN.
500	APIG.9003	Statistics Center request failed.	Statistics Center request failed.	Contact technical support.
500	APIG.9004	IAM request failed.	IAM request failed.	Contact technical support.
500	APIG.9005	VPC request failed.	VPC request failed.	Contact technical support.
500	APIG.9006	DNS request failed.	DNS request failed.	Contact technical support.
500	APIG.9007	ELB request failed.	ELB request failed.	Contact technical support.
500	APIG.9008	Too many requests. Try again later.	Too many requests. Try again later.	Please try again later.
500	APIG.9013	Synchronize CCMS data failed	Synchronize CCMS data failed	Contact technical support.
500	APIG.9999	Internal Server Error	Internal Server Error	Contact technical support.

7.5 Supported Features

The following table lists the features that are supported by **dedicated gateways**.

 NOTE

If the gateway you use does not have specific features, [submit a service ticket](#) to upgrade your gateway.

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
lts	Reporting of APIG gateway node access logs	Yes	{ "name": "lts", "enable": true, "config": { "group_id": " ", "topic_id": " ", "log_group": " ", "log_stream": " "} }	group_id	Log group ID.	-	-
				topic_id	Log stream ID.		
				log_group	Name of a log group.		
				log_stream	Name of a log stream.		
gateway_responses	Custom gateway responses	No	-	-	-	-	-

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
ratelimit	Request throttling limit configuration	Yes	<pre>{"name": "ratelimit", "enable": true, "config": {"api_limits": 500}}</pre>	api_limits	Default request throttling value applied to all APIs. Set this parameter properly to meet service requirements. A small value may constantly throttle your services.	200 calls per second	1–1,000,000 calls per second
request_body_size	Configuration of the maximum request body size	Yes	<pre>{"name": "request_body_size", "enable": true, "config": "104857600"}</pre>	request_body_size	Maximum size of the body allowed in an API request.	12 MB	1–9536 MB
backend_timeout	Maximum backend timeout configuration	Yes	<pre>{"name": "backend_timeout", "enable": true, "config": {"max_timeout": 500}}</pre>	max_timeout	Maximum timeout for APIG to request a backend service.	60,000 ms	1–600,000 ms

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
app_token	app_token authentication	Yes	{ "name": "app_token", "enable": true, "config": { "enable": "on", "app_token_expire_time": 3600, "app_token_uri": "/v1/apigw/oauth2/token", "refresh_token_expire_time": 7200 } }	enable	Whether to enable this feature.	Off	On/Off
				app_token_expire_time	Validity period of the access token.	3,600s	1–72,000s
				refresh_token_expire_time	Validity period of the refresh token.	7,200s	1–72,000s
				app_token_uri	URI used for obtaining the token.	/v1/apigw/oauth2/token	-
				app_token_key	Token encryption key.	-	-
app_api_key	app_api_key authentication	Yes	{ "name": "app_api_key", "enable": true, "config": "on" }	-	-	Off	On/Off
app_basic	app_basic authentication	Yes	{ "name": "app_basic", "enable": true, "config": "on" }	-	-	Off	On/Off

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
app_secret	app_secret authentication	Yes	{"name": "app_secret", "enable": true, "config": "on"}	-	-	Off	On/Off
app_jwt	app_jwt authentication	Yes	{"name": "app_jwt", "enable": true, "config": {"enable": "on", "auth_header": "Authorization"}}	enable	Whether to enable app_jwt authentication.	Off	On/Off
				auth_header	app_jwt authentication header.	Authorization	-
public_key	Public_key backed signatures	Yes	{"name": "public_key", "enable": true, "config": {"enable": "on", "public_key_uri_prefix": "/apigw/authadv/v2/public-key/"}}	enable	Whether to enable public_key authentication.	Off	On/Off
				public_key_uri_prefix	URI prefix used for obtaining the public key.	/apigw/authadv/v2/public-key/	-

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
backend_token_allow	Allowing tenants to transparently transmit tokens to the backend	Yes	<pre>{"name": "backend_token_allow", "enable": true, "config": {"backend_token_allow_users": [{"user_name": ""]}}</pre>	backend_token_allow_users	Regular expression for transparently transmitting the token to the common tenant whitelist of the tenant to match the domain name of the common tenant.	-	-
sign_basic	Basic signature keys	No	-	-	-	-	-
multi_auth	Two-factor authentication	No	-	-	-	-	-

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
backend_client_certificate	Backend two-way authentication	Yes	{ "name": "backend_client_certificate", "enable": true, "config": { "enable": " on ", "ca": " ", "content": " ", "key": " " } }	enable	Whether to enable this feature.	Off	On/Off
				ca	CA file of two-way authentication.	-	-
				content	Two-way authentication file.	-	-
				key	Private key of two-way authentication.	-	-

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
ssl_ciphers	HTTP S cipher suites	Yes	<pre>{"name": "ssl_ciphers", "enable": true, "config": "config": [{"ssl_ciphers\\": [\"ECDHE-ECDSA-AES256-GCM-SHA384\\\"]}]}</pre>	ssl_ciphers	Encryption and decryption suites supported. The ssl_ciphers parameter cannot be left blank and can contain only the options in the default value.	-	ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-SHA384, ECDHE-RSA-AES256-SHA384, ECDHE-ECDSA-AES128-SHA256, ECDHE-RSA-AES128-SHA256
route	Custom routes	No	-	-	-	-	-
cors	Plugins	No	-	-	-	-	-

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
real_ip_from_xff	X-Forwarded-For header for identifying IP addresses during access control and request throttling	Yes	<pre>{"name": "real_ip_from_xff", "enable": true, "config": {"enable": "on", "xff_index": -1}}</pre>	enable	Whether to enable this feature.	Off	On/Off

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
				xff_index	Sequence number of an IP address in the X-Forwarded-For header. The value of this parameter can be 0 or a positive or negative number. If the value is 0 or a positive number, the IP address of the corresponding index is obtained from the X-Forwarded-For header. If the value is a negative number, the IP address in reverse index order is obtained from the	-1	Valid Int32 value

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
					X-Forwarded-For header. For example, assume that the X-Forwarded-For header of a request received by API gateway contains three IP addresses: IP1, IP2, and IP3. If the value of xff_index is 0 , IP1 is obtained. If the value of xff_index is 1 , IP2 is obtained. If the value of xff_index is -1 , IP3 is obtained.		

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
app_route	IP address access	Yes	{"name": "app_route", "enable": true, "config": "on"}	-	-	Off	On/Off
vpc_name_modifiable	Load balance channel name modification	Yes	{"name": "vpc_name_modifiable", "enable": true, "config": "on"}	-	-	on	On/Off
default_group_host_trustlist	Access to the DEFAULT group from IP addresses that are not inbound access addresses of the current gateway	Yes	{"name": "default_group_host_trustlist", "enable": true, "config": "{ \"enable\": \"on\", \"hosts\": [\"123.2.2\", \"202.2.2\"] }"}	enable	Whether to enable this feature.	-	On/Off
				hosts	IP addresses that are not inbound access addresses of the current gateway.	-	-

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
throttle_strategy	Request throttling	Yes	{ "name": "throttle_strategy", "enable": true, "config": { "enable": " on ", "strategy": " local "} }	enable	Whether to enable this feature.	Off	On/Off
				strategy	Request throttling mode.	-	cluster/ local
custom_log	Printing custom request headers, query strings, and cookies in logs	Yes	{ "name": "custom_log", "enable": true, "config": { "custom_logs": [{ "location": " header ", "name": " a1234 "}] } }	custom_logs	Custom logs.	-	Max. 10 items.
				location	Location.		header/ query/ cookie
				name	Name.		-

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
real_ip_header_getter	Using a custom header to obtain source IP addresses	Yes	{ "name": "real_ip_header_getter", "enable": true, "config": { "enable": { "on": "\", \"header_getter\": \"header:testIP\" } } }	enable	Whether to enable this feature.	Off	On/Off
				header_getter	Custom header for obtaining source IP addresses.	-	-
policy_cookie_param	Using cookies in backend policy conditions	Yes	{ "name": "policy_cookie_param", "enable": true, "config": { "on": {} } }	-	-	Off	On/Off
app_quota	Client quotas	No	-	-	-	-	-
app_acl	Request throttling policies	No	-	-	-	-	-
set_resp_headers	Response header management plugins	No	-	-	-	-	-

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
vpc_backup	Primary/Standby VPC channels	No	-	-	-	-	-
sign_aes	AES signature keys	No	-	-	-	-	-
kafka_log	Adding, deleting, modifying, and querying Kafka log push plugins	No	-	-	-	-	-
backend_retry_count	Backend retry configuration	No	-	-	-	-	-
policy_sys_param	Using system parameters in backend policy conditions	No	-	-	-	-	-

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
breaker	Circuit breakers	No	-	-	-	-	-
content_type_configurable	Returning request parameter type (Content-Type) when querying APIs	No	-	-	-	-	-
rate_limit_plugin	Request throttling plugins	No	-	-	-	-	-
breakerv2	Circuit breakers for degrading services in case of overload	No	-	-	-	-	-

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
sm_cipher_type	Encrypting local sensitive data with commercial cryptographic algorithms	No	-	-	-	-	-
rate_limit_algorithm	Request throttling algorithm switch over	No	-	-	-	-	-
gzip	Response compression using gzip	Yes	{ "name": "gzip", "config": { "comp_level": 6, "enable": true } }	comp_level	gzip compression level (1 to 9). The higher the level, the more compressed but takes a longer time.	6	1–9

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
sse_strategy	SSE transmission	Yes	{ "name": "sse_strategy", "enable": true, "config": "on" }	-	-	Off	On/Off
authorizer_context_support_num_bool	Whether the value of the key-value pair in the context returned for custom authentication can be a number or Boolean value.	No	-	-	-	-	-

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
custom_auth_header	Custom authentication headers for app authentication and signature key policies.	Yes	1: { "name": "custom_auth_header", "enable": true, "config": {"app_auth_header": "\: \"app-header \", \"backend_sign_header \", \"back-header \", \"}\" }	app_auth_header	Used to specify the signature information for app authentication in the request header.	-	Leave this parameter blank, or enter 3 to 64 letters, digits, hyphens (-), and underscores (_), and start with a letter. Do not start with x-apig- or x-sdk- , and do not use x-stage or authorization . The value is case-insensitive.
				backend_sign_header	Used to specify the signature information of signature key policies (Basic, Auth, HMAC) to pass to the backend.	-	

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
request_custom_config	Configuring client request parameters	Yes	{ "name": "request_custom_config" , "enable": true, "config": :{ "http2\":"on" }, "client_body_timeout\":"10" } }	http2	Whether to enable HTTP/2.	on	On/Off
				client_body_timeout	Client request body timeout.	8s	1-60s
gateway_responses_support_header	Custom group response supports custom header.	No	-	-	-	-	-
api_uri_no_escape	Unescaping request parameters of the request path in the API.	Yes	{"name": "api_uri_no_escape", "enable": true, "config": ""}	enable	Whether to enable this feature.	false	true/false

Feature Name	Feature Description	Configurable	Feature Configuration Example	Configuration Parameter	Parameter Description	Default Value	Value Range
ip_control	Access control	Yes	{ "enable": true, "name": "ip_control", "config": { "control_type": "\white", "white_ip_list": "\", \"white_ip_list", "black_ip_list": "\", \"black_ip_list", "black_ip_list": "\", \"black_ip_list" } }	control_type	Control type.	black	black/white
				white_ip_list	IP address whitelist.	-	-
				black_ip_list	IP address blacklist.	-	-
kafka_log_plugin_options	Customizing message size through Kafka log push plugin.	Yes	{ "name": "kafka_log_plugin_options", "enable": true, "config": { "request_body_size": 1000, "response_body_size": 1000 } }	request_body_size	Custom request body size, in bytes.	1000	1000-4096
				response_body_size	Custom response body size, in bytes.	1000	1000-4096

7.6 Obtaining a Project ID

Calling an API

You can also call the API used to **query project information** to obtain a project ID.

The API used to obtain a project ID is "GET https://{Endpoint}/v3/projects/". {Endpoint} is the IAM endpoint and can be obtained from [Regions and Endpoints](#). For details on API calling authentication, see [Authentication](#).

The following is an example response. The value of **id** in the **projects** field is the project ID.

```
{
  "projects": [
    {
      "domain_id": "65382450e8f64ac0870cd180d14e684b",
      "is_domain": false,
      "parent_id": "65382450e8f64ac0870cd180d14e684b",
      "name": "xx-north-4",
      "description": "",
      "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
      },
      "id": "a4a5d4098fb4474fa22cd05f897d6b99",
      "enabled": true
    }
  ],
  "links": {
    "next": null,
    "previous": null,
    "self": "https://www.example.com/v3/projects"
  }
}
```

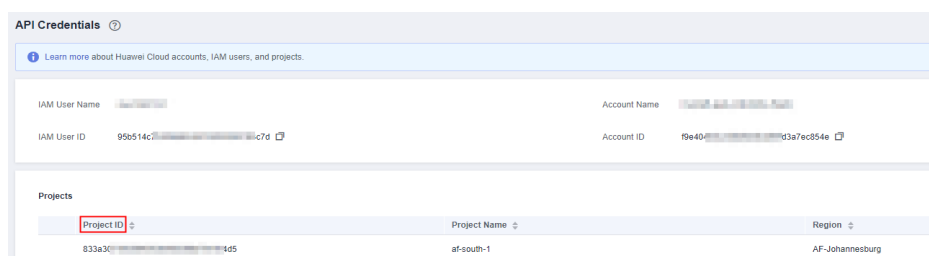
Obtaining a Project ID on the Console

A project ID needs to be specified in the URLs of some APIs. Therefore, you need to obtain a project ID before calling such APIs. To obtain a project ID, perform the following operations:

1. Log in to the management console.
2. Hover the mouse pointer over the username and choose **My Credentials** from the drop-down list.

On the API Credentials page, view project IDs in the project list.

Figure 7-1 Viewing project IDs



If there are multiple projects in one region, expand **Region** and view subproject IDs in the **Project ID** column.

7.7 Obtaining an Account Name and Account ID

An account name and account ID are required for some URLs when an API is called. To obtain an account name and account ID, perform the following operations:

1. Log in to the management console.
2. Hover the mouse pointer over the username and choose **My Credentials** from the drop-down list.

View the account name and account ID.

7.8 Data Structure (Plugin Content Definition)

7.8.1 CorsPluginContent

Table 7-2 CorsPluginContent

Parameter	Mandatory	Type	Description
allow_origin	Yes	String	Access-Control-Allow-Origin header, which specifies the origins that are allowed to access the resource. For requests that do not need to carry an identity credential, enter an asterisk (*) to allow requests from all origins. Separate multiple domain names using commas.
allow_methods	No	String	The Access-Control-Allow-Methods header specifies the HTTP methods allowed when accessing the resource. Use commas (,) to separate multiple methods.
allow_headers	No	String	Access-Control-Allow-Headers header, which specifies the header fields that can be carried in a request. Use commas (,) to separate multiple header fields.

Parameter	Mandatory	Type	Description
expose_headers	No	String	The Access-Control-Expose-Headers header lets a server whitelist headers that browsers are allowed to access. Use commas (,) to separate multiple header fields.
max_age	No	Integer	Access-Control-Max-Age header, which specifies how long the results of a preflight request can be cached. Value range: 0s to 86,400s. No more preflight requests are needed within the period.
allow_credentials	No	Boolean	Access-Control-Allow-Credentials header, which specifies whether to allow the browser to read the response content.

7.8.2 SetRespHeadersContent

Table 7-3 SetRespHeadersContent

Parameter	Mandatory	Type	Description
response_headers	No	Array of HeaderPolicy objects	Response header information.

Table 7-4 HeaderPolicy

Parameter	Mandatory	Type	Description
name	No	String	Response header name, which is case-insensitive. Start with a letter, and include letters, digits, and hyphens (-). (1 to 32 characters)

Parameter	Mandatory	Type	Description
value_type	No	String	Default value. If this parameter is not specified, the default value is the custom content. Options: • custom_value: Use the custom content as the value. • system_parameter: Use a system parameter as the value.
value	No	String	Response header value, with a maximum of 255 characters. When value_type is set to a system parameter, gateway system parameters can be used. The gateway system parameter is as follows: • \$context.cacheStatus: response cache hit status.
action	No	String	Action to be executed by the plug-in when the backend response contains this response header. The value can be append, override, delete, skip, or add. The value is case insensitive. When the value type is a system parameter, only add and append can be selected.

7.8.3 KafkaLogContent

Table 7-5 KafkaLogContent

Parameter	Mandatory	Type	Description
broker_list	Yes	Array of strings	Broker addresses of the target Kafka.
topic	Yes	String	Topic of the logs reported by the target Kafka.
key	No	String	Key allocated to the message partition.

Parameter	Mandatory	Type	Description
max_retry_count	No	Integer	Number of attempts to resend a message after it fails to be sent. Default value: 0. Range: 0–5.
retry_backoff	No	Integer	Interval between resending attempts, in seconds. Value range: 1–10.
sasl_config	No	PluginKafkaLogSaslConfig object	SASL configuration of the Kafka log push plug-in.
meta_config	No	PluginKafkaLogMetaConfig object	Metadata configuration of the Kafka log push plug-in.

Table 7-6 PluginKafkaLogSaslConfig

Parameter	Mandatory	Type	Description
security_protocol	No	String	Security protocol. Default value: PLAINTEXT. Options: - PLAINTEXT: user authentication protocol of the default access point. - SASL_PLAINTEXT: SASL user authentication protocol. - SASL_SSL: SSL user authentication protocol.
sasl_mechanisms	No	String	Message transmission and receiving mechanism. The default value is PLAIN.
sasl_username	No	String	SASL username. This parameter is required when security_protocol is set to SASL_PLAINTEXT or SASL_SSL. Ignore this parameter when security_protocol is set to PLAINTEXT.

Parameter	Mandatory	Type	Description
sasl_password	No	String	SASL password. This parameter is required when security_protocol is set to SASL_PLAINTEXT or SASL_SSL. Ignore this parameter when security_protocol is set to PLAINTEXT.
ssl_ca_content	No	String	CA certificate content. This parameter is required when security_protocol is set to SASL_SSL.

Table 7-7 PluginKafkaLogMetaConfig

Parameter	Mandatory	Type	Description
system	No	PluginKafkaLogMetaSystem object	System configuration for Kafka log metadata.
call_data	No	PluginKafkaLogMetaCallData object	Metadata invocation data of the Kafka log push plug-in.

Table 7-8 PluginKafkaLogMetaSystem

Parameter	Mandatory	Type	Description
start_time	No	Boolean	Whether to report the Kafka request start time (Unix timestamp). The default value is true.
request_id	No	Boolean	Whether to report the Kafka request ID. The default value is true.
client_ip	No	Boolean	Whether to report the Kafka client IP address. The default value is true.
api_id	No	Boolean	Whether to report the Kafka API ID.
user_name	No	Boolean	Whether to report the Kafka username.

Parameter	Mandatory	Type	Description
app_id	No	Boolean	Whether to report the Kafka app ID.
request_time	No	Boolean	Whether to report the Kafka request duration (second). The default value is true.
http_status	No	Boolean	Whether to report the Kafka response code. The default value is true.
server_protocol	No	Boolean	Whether to report the Kafka request protocol version (HTTP/1.0 or HTTP/1.1).
scheme	No	Boolean	Whether to report the Kafka request protocol (HTTP or HTTPS). The default value is true.
request_method	No	Boolean	Whether to report the Kafka request method. The default value is true.
host	No	Boolean	Whether to report the Kafka request host (IP:PORT or Domain_name:PORT). The default value is true.
api_uri_mode	No	Boolean	Whether to report the Kafka request matching mode (NORMAL or SWA).
uri	No	Boolean	Whether to report the Kafka request URI. The default value is true.
request_size	No	Boolean	Whether to report the Kafka request size (byte).
response_size	No	Boolean	Whether to report the Kafka response size (byte).
upstream_uri	No	Boolean	Whether to report the Kafka backend URI.
upstream_address	No	Boolean	Whether to report the Kafka backend address. The default value is true.
upstream_status	No	Boolean	Whether to report the Kafka backend response code. The default value is true.

Parameter	Mandatory	Type	Description
upstream_connect_time	No	Boolean	Whether to report the Kafka backend connection time (second).
upstream_header_time	No	Boolean	Whether to report the time (second) spent returning the Kafka backend response header.
upstream_response_time	No	Boolean	Whether to report the Kafka backend response duration (second). The default value is true.
http_x_forwarded_for	No	Boolean	Whether to report the content of x_forwarded_for in the Kafka request. The default value is true.
http_user_agent	No	Boolean	Whether to report the proxy of the Kafka request. The default value is true.
region_id	No	Boolean	Whether to report the region ID of Kafka.
all_upstream_response_time	No	Boolean	Whether to report the time (second) spent receiving all bytes, including the time of retry attempts.
error_type	No	Boolean	Whether to report the Kafka request error type, which can be 0 (non-request throttling) or 1 (request throttling). The default value is true.
auth_type	No	Boolean	Whether to report the API authentication mode of the Kafka request.
access_model_1	No	Boolean	Whether to report authentication mode 1 of the Kafka request.
access_model_2	No	Boolean	Whether to report authentication mode 2 of the Kafka request. The custom authorizer ID is used for two-factor authentication.
inner_time	No	Boolean	Whether to report the internal processing time (second) of the Kafka request.

Parameter	Mandatory	Type	Description
proxy_protocol_vni	No	Boolean	Whether to report the virtual network identifier (VNID) in VPCEP for the Kafka request.
proxy_protocol_vpce_id	No	Boolean	Whether to report the VPCEP ID of the Kafka request.
proxy_protocol_addr	No	Boolean	Whether to report the PP2 address of the Kafka request.
body_bytes_sent	No	Boolean	Whether to report the body size of the Kafka request.
api_name	No	Boolean	Whether to report the API name of the Kafka request.
app_name	No	Boolean	Whether to report the app name of the Kafka request.
provider_app_id	No	Boolean	Whether to report the ID of the app to which the API called by the Kafka request belongs.
provider_app_name	No	Boolean	Whether to report the name of the app to which the API called by the Kafka request belongs.
custom_data_log01	No	Boolean	Whether to report reserved log field 01 customized by the Kafka client.
custom_data_log02	No	Boolean	Whether to report reserved log field 02 customized by the Kafka client.
custom_data_log03	No	Boolean	Whether to report reserved log field 03 customized by the Kafka client.
custom_data_log04	No	Boolean	Whether to report reserved log field 04 customized by the Kafka client.
custom_data_log05	No	Boolean	Whether to report reserved log field 05 customized by the Kafka client.
custom_data_log06	No	Boolean	Whether to report reserved log field 06 customized by the Kafka client.

Parameter	Mandatory	Type	Description
custom_data_log07	No	Boolean	Whether to report reserved log field 07 customized by the Kafka client.
custom_data_log08	No	Boolean	Whether to report reserved log field 08 customized by the Kafka client.
custom_data_log09	No	Boolean	Whether to report reserved log field 09 customized by the Kafka client.
custom_data_log10	No	Boolean	Whether to report reserved log field 10 customized by the Kafka client.
response_source	No	Boolean	Whether to report the Kafka response source. The response source can be local (API gateway) or remote (backend service).

Table 7-9 PluginKafkaLogMetaCallData

Parameter	Mandatory	Type	Description
log_request_header	No	Boolean	Whether logs include request headers. The default value is false, indicating that request headers are not included.
request_header_filter	No	String	Request header fields that can be included in logs. Separate them with commas (,), and use wildcard characters (*) if necessary.
log_request_query_string	No	Boolean	Whether logs include query strings. The default value is false, indicating that query strings are not included.
request_query_string_filter	No	String	Query strings that can be included in logs. Separate them with commas (,), and use wildcard characters (*) if necessary.

Parameter	Mandatory	Type	Description
log_request_body	No	Boolean	Whether logs include the request body. The default value is false, indicating that the request body is not included.
log_response_header	No	Boolean	Whether logs include response headers. The default value is false, indicating that response headers are not included.
response_header_filter	No	String	Response header fields that can be included in logs. Separate them with commas (,), and use wildcard characters (*) if necessary.
log_response_body	No	Boolean	Whether logs include the response body. The default value is false, indicating that the response body is not included.
custom_authORIZER	No	PluginKafkaLogMetaAuthORIZER object	Authentication configuration for Kafka log metadata.

Table 7-10 PluginKafkaLogMetaAuthorizer

Parameter	Mandatory	Type	Description
frontend	No	Array of strings	Log fields in the response of custom frontend authentication.
backend	No	Array of strings	Log fields in the response of custom backend authentication.

7.8.4 BreakerContent

Table 7-11 BreakerContent

Parameter	Mandatory	Type	Description
scope	No	String	Circuit breaker plug-in type. Options: • basic: APIs bound with the plug-in are calculated separately for circuit breaker triggering. • share: APIs bound with the plug-in are calculated together for circuit breaker triggering.
breaker_condition	Yes	PluginBreakerCondition object	Circuit breaker plug-in condition.
downgrade_default	No	PluginBreakerDowngradeInfo object	Backend definition for the downgrade policy of the circuit breaker plug-in.
downgrade_parameters	No	Array of PluginCommonParameter objects	Circuit breaker rule parameters.
downgrade_rules	No	Array of PluginBreakerDowngradeRule objects	Downgrade rules of the circuit breaker.

Table 7-12 PluginBreakerDowngradeRule

Parameter	Mandatory	Type	Description
rule_name	Yes	String	Circuit breaker rule name.
match_regex	Yes	String	Circuit breaker rule expression. For details, see the rule expression description.
breaker_condition	No	PluginBreakerCondition object	Circuit breaker plug-in condition.
downgrade_backend	No	PluginBreakerDowngradeInfo object	Backend definition for the downgrade policy of the circuit breaker plug-in.

Parameter	Mandatory	Type	Description
parameters	No	Array of PluginCommonParameter objects	Circuit breaker rule parameters.

Table 7-13 PluginBreakerCondition

Parameter	Mandatory	Type	Description
breaker_type	Yes	String	Circuit breaker type. Options: • timeout: Backend timeout circuit breaker. • condition: Backend condition-based circuit breaker.
breaker_mode	No	String	Circuit breaker condition type. Options: • counter • percentage
unhealthy_condition	No	String	Rule expression. For details, see the rule expression description.
unhealthy_threshold	No	Integer	Number of requests to trigger unhealthy conditions. This parameter is required when breaker_mode is set to counter.
min_call_threshold	No	Integer	Minimum number of requests to trigger the circuit breaker. This parameter is required when breaker_mode is set to percentage.
unhealthy_percentage	No	Integer	Minimum percentage of unhealthy conditions to trigger the circuit breaker. This parameter is required when breaker_mode is set to percentage.
time_window	Yes	Integer	Time window for determining the number of unhealthy times. The unit is second.

Parameter	Mandatory	Type	Description
open_breaker_time	Yes	Integer	Duration for which the circuit breaker is on. The unit is second.

Table 7-14 PluginBreakerDowngradeInfo

Parameter	Mandatory	Type	Description
type	Yes	String	Circuit breaker downgrade type: http, http_vpc, function, mock, or passthrough. Options: • http: HTTP backend. • http_vpc: HTTP load balancer. • function: function backend. • mock: Mock backend. • passthrough: passthrough parameters.
http_info	No	PluginBreakerDowngradeHttpInfo object	HTTP backend definition for the downgrade policy of the circuit breaker plug-in.
http_vpc_info	No	PluginBreakerDowngradeHttpVpcInfo object	HTTP backend load balancing definition for the downgrade policy of the circuit breaker plug-in.
func_info	No	PluginBreakerDowngradeFunctionInfo object	Function backend definition for the downgrade policy of the circuit breaker plug-in.
mock_info	No	PluginBreakerDowngradeMockInfo object	Mock backend definition for the downgrade policy of the circuit breaker plug-in.
passthrough_infos	No	Array of PluginBreakerDowngradePassthroughInfo objects	This parameter is required when the circuit breaker downgrade type is set to "passthrough".

Table 7-15 PluginBreakerDowngradeHttpInfo

Parameter	Mandatory	Type	Description
address	Yes	String	Backend service address. It consists of a domain name or IP address and a port number. Maximum length: 255 characters. It must be in the format "Host name:Port number", for example, apig.example.com:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used.
scheme	Yes	String	Request protocol. Options: • HTTP • HTTPS
method	Yes	String	Request method. Options: • GET • POST • PUT • DELETE • HEAD • PATCH • OPTIONS • ANY
path	Yes	String	Request address. The request path can contain a maximum of 512 characters with request parameters enclosed in braces {}, for example, / getUserInfo/{userId} , and these special characters: */%_-. NOTE The value of this parameter must comply with URI specifications.
timeout	Yes	Integer	Timeout allowed for requesting the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms.

Table 7-16 PluginBreakerDowngradeHttpVpcInfo

Parameter	Mandatory	Type	Description
vpc_channel_id	Yes	String	Load balance channel ID.
scheme	Yes	String	Request protocol. Options: • HTTP • HTTPS
method	Yes	String	Request method.
path	Yes	String	Request address. The request path can contain a maximum of 512 characters with request parameters enclosed in braces ({}), for example, / getUserInfo/{userId} , and these special characters: */%-. NOTE The value of this parameter must comply with URI specifications.
timeout	Yes	Integer	Timeout allowed for requesting the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms.

Table 7-17 PluginBreakerDowngradeFunctionInfo

Parameter	Mandatory	Type	Description
function_urn	Yes	String	Function URN.
version	No	String	Version. Either alias or version must be set.
alias_urn	No	String	Alias. Either alias or version must be set.
invocation_type	Yes	String	Invocation mode. Options: • async: asynchronous • sync: synchronous

Parameter	Mandatory	Type	Description
timeout	Yes	Integer	Timeout allowed for requesting the backend service. You can set the maximum timeout using the backend_timeout configuration item. The maximum value is 600,000. Unit: ms.

Table 7-18 PluginBreakerDowngradeMockInfo

Parameter	Mandatory	Type	Description
status_code	Yes	String	HTTP status code for the Mock backend. Options: • 200: OK • 201: Created • 202: Accepted • 203: NonAuthoritativeInformation • 204: NoContent • 205: ResetContent • 206: PartialContent • 300: MultipleChoices • 301: MovedPermanently • 302: Found • 303: SeeOther • 304: NotModified • 305: UseProxy • 306: Unused • 307: TemporaryRedirect • 400: BadRequest • 401: Unauthorized • 402: PaymentRequired • 403: Forbidden • 404: NotFound • 405: MethodNotAllowed • 406: NotAcceptable • 407: ProxyAuthentication-Required • 408: RequestTimeout • 409: Conflict • 410: Gone • 411: LengthRequired • 412: PreconditionFailed • 413: RequestEntityTooLarge • 414: RequestURITooLong • 415: UnsupportedMedia-Type • 416: RequestedRangeNot-Satisfiable • 417: ExpectationFailed

Parameter	Mandatory	Type	Description
			• 450: ParameterRequired • 451: MethodConnectException • 500: InternalServerError • 501: NotImplemented • 502: BadGateway • 503: ServiceUnavailable • 504: GatewayTimeout • 505: HTTPVersionNotSupported
result_content	No	String	Response body.
headers	No	Array of PluginBreakerDowngradeMockHeader objects	Mock response header.

Table 7-19 PluginBreakerDowngradeMockHeader

Parameter	Mandatory	Type	Description
key	No	String	Response header name.
value	Yes	String	Response header value.

Table 7-20 PluginBreakerDowngradePassthroughInfo

Parameter	Mandatory	Type	Description
location	No	String	Parameter location: header, query, or path.
name	Yes	String	Parameter name. Start with a letter and include only letters, digits, hyphens (-), underscores (_), and periods (.).
origin	Yes	String	Parameter type: constant or system.

Parameter	Mandatory	Type	Description
value	Yes	String	Parameter value with a maximum of 255 characters. If the origin type is "constant", the value is a constant. If the origin type is "system", the value is a system parameter name. System parameters include gateway parameters and frontend/backend authentication parameters. You can set the frontend or backend authentication parameters after enabling custom frontend or backend authentication. The gateway parameters are as follows: • <code>\$context.sourcelp</code>: source IP address of the API caller • <code>\$context.stage</code>: deployment environment in which the API is called • <code>\$context.apiName</code>: API name. • <code>\$context.apild</code>: API ID • <code>\$context.appName</code>: name of the app used by the API caller. • <code>\$context.appld</code>: ID of the app used by the API caller • <code>\$context.requestId</code>: request ID generated when the API is called • <code>\$context.serverAddr</code>: address of the gateway server • <code>\$context.serverName</code>: name of the gateway server • <code>\$context.handleTime</code>: processing time of the API request • <code>\$context.providerAppId</code>: ID of the app used by the API owner (not supported) Frontend authentication parameter: prefixed with

Parameter	Mandatory	Type	Description
			"\$context.authorizer.frontend." . For example, to return "aaa" upon successful custom authentication, set this parameter to "\$context.authorizer.frontend.a aa". Backend authentication parameter: prefixed with "\$context.authorizer.backend." For example, to return "aaa" upon successful custom authentication, set this parameter to "\$context.authorizer.backend.a aa".

Table 7-21 PluginCommonParameter

Parameter	Mandatory	Type	Description
type	Yes	String	Parameter type. Options: • header: the value of the first HTTP header with the parameter name you set. • query: the value of the first query string with the parameter name you set. • path: complete HTTP request path. • method: HTTP request method. • system: system parameter.
name	Yes	String	Parameter name for "parameters" of "rules".
value	Yes	String	Parameter source value.

7.8.5 RateLimitContent

Table 7-22 RateLimitContent

Parameter	Mandatory	Type	Description
scope	No	String	Type of the request throttling policy. • basic: Limit the maximum number of times a single API bound with the policy can be called within the specified period. • share: Limit the maximum number of times all APIs bound with the policy can be called within the specified period.
default_time_unit	No	String	Time unit for limiting the number of API calls. Default unit: second. • second • minute • hour • day
default_interval	No	Integer	Period of time for limiting the number of API calls. This parameter applies with each of the preceding three API call limits. This value must be a positive integer and cannot exceed 2,147,483,647.
api_limit	Yes	Integer	Maximum number of times an API can be accessed within a specified period. The value cannot exceed the default quota limit. This value must be a positive integer and cannot exceed 2,147,483,647 or -1. -1 indicates that no request throttling is applied.

Parameter	Mandatory	Type	Description
app_limit	No	Integer	Maximum number of times the API can be accessed by an app within the same period. The value of this parameter must be less than or equal to that of user_call_limits . This value must be a positive integer and cannot exceed 2,147,483,647.
user_limit	No	Integer	Maximum number of times the API can be accessed by a user within the same period. The value of this parameter must be less than or equal to that of api_call_limits . This value must be a positive integer and cannot exceed 2,147,483,647.
ip_limit	No	Integer	Maximum number of times the API can be accessed by an IP address within the same period. The value of this parameter must be less than or equal to that of api_call_limits . This value must be a positive integer and cannot exceed 2,147,483,647.
algorithm	No	String	Throttling type. Options: • counter: High-precision throttling. • haht: High-performance throttling. • local: Single-node throttling.
specials	No	Array of RateLimitSpecial objects	Excluded configurations for basic throttling.
parameters	No	Array of PluginCommonParameter objects	Parameters for parameter-based throttling.
rules	No	Array of RateLimitRule objects	Rules for parameter-based throttling.

Table 7-23 RateLimitSpecial

Parameter	Mandatory	Type	Description
type	Yes	String	Type of the request throttling policy. Options: • app: application • user: IAM tenant
policies	Yes	Array of RateLimitSpecialPolicy objects	Excluded request throttling policies.

Table 7-24 RateLimitSpecialPolicy

Parameter	Mandatory	Type	Description
key	Yes	String	Object of excluded request throttling.
limit	Yes	Integer	Maximum number of times an excluded object can access an API within the throttling period. The value cannot exceed api_limit.

Table 7-25 PluginCommonParameter

Parameter	Mandatory	Type	Description
type	Yes	String	Parameter type. Options: • header: the value of the first HTTP header with the parameter name you set. • query: the value of the first query string with the parameter name you set. • path: complete HTTP request path. • method: HTTP request method. • system: system parameter.
name	Yes	String	Parameter name for "parameters" of "rules".
value	Yes	String	Parameter source value.

Table 7-26 RateLimitRule

Parameter	Mandatory	Type	Description
rule_name	Yes	String	Request throttling policy rule name.
match_regex	Yes	String	Rule expression. For details, see the rule expression description.
time_unit	No	String	Time unit for limiting the number of API calls. Default unit: value of default_time_unit. Options: • second • minute • hour • day
interval	No	Integer	Interval for limiting the number of API calls. Default unit: value of default_interval.
limit	Yes	Integer	Throttling limit, which is a positive integer. -1 indicates that request throttling is not required when this limited is reached.

7.8.6 ThirdAuthContent

Table 7-27 ThirdAuthContent

Parameter	Mandatory	Type	Description
auth_request	No	PluginThirdAuthRequest object	Authentication API information.
identities	No	PluginThirdAuthIdentities object	User identity authentication information.
carry_body	No	PluginThirdAuthCarryBody object	Whether to allow the API request body for third-party authentication.
carry_path_enabled	No	Boolean	Whether to allow original request path.

Parameter	Mandatory	Type	Description
return_resp_body_enabled	No	Boolean	Whether to return response.
carry_resp_header	No	Array of strings	Allowed response header. (If third-party authentication is successful, this header will be obtained from the response header of the authentication API and then transparently transmitted to the backend. A maximum of 10 parameters are allowed. The parameter length is from 1 to 64 characters.)
simple_auth_mode_enabled	No	Boolean	Simple authentication. (Status codes starting with "2" indicate the authentication is successful.)
match_auth	No	PluginThirdAuthMatchAuth object	Authentication result matching.
rule_enabled	No	Boolean	Whether to enable the blacklist/whitelist function. (APIs verified by the blacklist/whitelist will not be authenticated with the authentication API.)
rule_type	No	String	Blacklist/Whitelist type. This parameter is mandatory when the blacklist/whitelist function is enabled.
parameters	No	Array of PluginThirdAuthParameters objects	Blacklist/Whitelist rule parameters.
rules	No	Array of PluginThirdAuthRule objects	Blacklist/Whitelist parameter verification rules. A maximum of 100 rules are allowed.

Parameter	Mandatory	Type	Description
custom_forbid_limit	No	Integer	Anti-brute force cracking threshold. (If the number of authentication attempts within 5 minutes exceeds this threshold, requests will be blocked and the authentication will fail until the next 5-minute window starts.)
auth_downgrade_enabled	No	Boolean	Relaxed mode. (The gateway receives requests from clients even if the authentication service cannot be connected or returns an error code starting with "5".)

Table 7-28 PluginThirdAuthRequest

Parameter	Mandatory	Type	Description
method	Yes	String	Authentication API request method.
protocol	Yes	String	Authentication API request protocol (HTTP not recommended).
url_domain	No	String	Authentication API address. This parameter is mandatory when no load balance channel is used. Use an IP address or a domain name, with up to 255 characters.
timeout	No	Integer	Authentication API timeout in seconds. Range: 1 ms to 60,000 ms. Default: 5,000 ms.
path	Yes	String	Authentication API path. Start with a slash (/) and use letters, digits, underscores (_), and hyphens (-). The path can contain query strings.
vpc_channel_enabled	Yes	Boolean	Whether to use a load balance channel. true: yes; false: no.
vpc_channel_info	No	PluginThirdAuthVpcChannelInfo object	Load balance channel information.

Table 7-29 PluginThirdAuthVpcChannelInfo

Parameter	Mandatory	Type	Description
vpc_id	Yes	String	Load balance channel ID.
vpc_proxy_host	No	String	Custom host header, a domain name that contains 1 to 254 characters, including letters, digits, periods (.), colons, and hyphens (-).

Table 7-30 PluginThirdAuthIdentities

Parameter	Mandatory	Type	Description
headers	No	Array of PluginThirdAuthIdentity objects	Request headers. A maximum of 10 request headers are allowed.
queries	No	Array of PluginThirdAuthIdentity objects	Query strings. A maximum of 10 query strings are allowed.

Table 7-31 PluginThirdAuthIdentity

Parameter	Mandatory	Type	Description
name	Yes	String	Start with a letter, and use letters, digits, periods (.), underscores (_), and hyphens (-). (1 to 32 characters)

Table 7-32 PluginThirdAuthCarryBody

Parameter	Mandatory	Type	Description
enabled	Yes	Boolean	true: yes; false: no.
max_body_size	No	Integer	Maximum number of bytes that are allowed. It cannot exceed the maximum body size allowed in a request.

Table 7-33 PluginThirdAuthMatchAuth

Parameter	Mandatory	Type	Description
key	Yes	String	Key in the authentication response header. (1 to 64 characters)
value	Yes	String	Value in the authentication response header. (1 to 512 characters)

Table 7-34 PluginThirdAuthParameters

Parameter	Mandatory	Type	Description
type	Yes	String	Parameter type. Options: • header: the value of the first HTTP header with the parameter name you set. • query: the value of the first query string with the parameter name you set. • path: complete HTTP request path. • method: HTTP request method. • system: system parameter.
name	Yes	String	Parameter name. Set path to reqPath, method to method, header and query to the header and query parameter key, and system to any of [sourcelp,stage,apild,appld,requestId,serverAddr,serverName,handleTime,providerAppld,apiName,appName,authorizer.frontend.xx,authorizer.backend.xx].
value	Yes	String	Parameter source value.

Table 7-35 PluginThirdAuthRule

Parameter	Mandatory	Type	Description
rule_name	Yes	String	Name of a parameter verification rule. The name must start with a letter or digit, followed by letters, digits, colons (:), periods (.), underscores (_), parentheses (()), and slashes (/). It cannot start or end with a space. (2 to 254 characters)
match_regex	Yes	String	Parameter verification rule. A rule is indicated by [] and consists of a parameter name, matching rule (== (equal to), ~= (not equal to), in (enumerated value), ~~ (regular expression)), and matching value. Square brackets can be nested in [] and connected by OR or AND at the same level. The following example indicates that the verification is passed if the Host parameter in the header matches the regular expression ^f0269b2874ef0b65bee1f314e52aa.*\$, or the request path is /a, /b, /returnRequest, or /d.

7.8.7 ProxyCacheContent

Table 7-36 ProxyCacheContent

Parameter	Mandatory	Type	Description
cache_key	No	PluginProxyCacheKey object	The configuration parameter is used as the value of the cache proxy key. cache_key is mandatory. Therefore, at least one of the system_params , parameters , and headers parameters needs to be configured.

Parameter	Mandatory	Type	Description
cache_http_status_and_ttl	No	Array of PluginProxyCacheHttpStatusTtl objects	HTTP status codes that can be cached and the cache duration.
client_cache_control	No	PluginProxyCacheClientCacheControl object	Allows the client to use the Cache-Control header to affect the cache policy.
cacheable_headers	No	Array of strings	Backend headers that can be cached. By default, only the Content-Type, Content-Encoding, and Content-Language headers are cached. A maximum of 20 parameters are supported. The value is a string of 1 to 64 characters. System response headers (such as x-apig-* and x-request-id) added by APIG cannot be added.

Table 7-37 PluginProxyCacheKey

Parameter	Mandatory	Type	Description
system_parameters	No	Array of strings	The built-in system parameter of the gateway is used as the value of the cache proxy key. The gateway parameters are as follows: • \$context.sourceIp: source IP address of the API caller • \$context.stage: deployment environment in which the API is called • \$context.apiId: API ID • \$context.appId: ID of the app used by the API caller • \$context.requestId: request ID generated when the API is called. • \$context.serverAddr: address of the gateway server • \$context.serverName: name of the gateway server • \$context.handleTime: processing time of the API request • \$context.providerAppId: ID of the app used by the API owner (not supported) • \$context.apiName: API name, which can be used only after the API is published • \$context.appName: name of the credential used for calling the API
parameters	No	Array of strings	The request query parameter is used as the value of the cache proxy key.
headers	No	Array of strings	The request header is used as the value of the cache proxy key.

Table 7-38 PluginProxyCacheHttpStatusTtl

Parameter	Mandatory	Type	Description
http_status	No	Array of integers	Determines whether to cache content based on the HTTP response code.
ttl	No	Integer	Cache expiration time, in seconds.

Table 7-39 PluginProxyCacheClientCacheControl

Parameter	Mandatory	Type	Description
mode	No	String	Mode in which the client is allowed to affect the cache policy. Options: • off: rejects all requests. • all: allows all requests. • apps: The value of App ID can be in the datas list.
datas	No	Array of strings	If mode is set to apps, values of App ID in the following table are allowed.

7.8.8 ProxyMirrorContent

Table 7-40 ProxyMirrorContent

Parameter	Mandatory	Type	Description
protocol	Yes	String	The image request protocol.
host	Yes	String	The image service address, which consists of the IP address/domain name and port number. Max.: 255 characters. Format: Host name:Port number. Example: xxx.xxx.xxx:7443. If the port number is not specified, the default HTTPS port 443 or the default HTTP port 80 is used.

Parameter	Mandatory	Type	Description
path	No	String	URI for non-gRPC image requests. If this parameter is not specified, the original request path is used by default. The path can contain special characters (*%-.). It can contain a maximum of 512 characters and must comply with URI specifications. NOTE The value of this parameter must comply with URI specifications.
path_concat_mode	No	String	Specifies how to concatenate the image request (non-gRPC) path. Replace (default): Uses the specified request path; Prefix: Combines the specified path and the source request URI.
sample_ratio	No	Float	Sampling rate of the image request. Default: 1 (full sampling)
timeout	No	Integer	Image request timeout. Unit: ms.
mirror_request_body_enabled	No	Boolean	Mirrors the body of client requests. Enabled by default.

8 Change History

Table 8-1 Change history

Released On	Change History
2025-04-19	Updated APIs Added the trace_enabled parameter to the APIs for creating an API, modifying an API, querying API details, querying APIs, querying the API runtime definition, and querying API version details.
2025-12-10	Updated APIs Added the third_authorizer_param_name parameter to the APIs for creating an API, modifying an API, querying API details, and querying API version details.
2024-06-26	- Added descriptions about orchestration rule management APIs. - Added descriptions about gateway custom inbound port management APIs.
2024-01-19	- Added the API for querying the supported features of a gateway. - Added the API for setting accessibility of a debugging domain name. - Added the API for managing asynchronous tasks.

Released On	Change History
2023-09-12	- Added the API for modifying a variable. - Added the API for verifying the definition of an API. - Modified descriptions of the API for creating a pay-per-use gateway. - Added the API for modifying the specifications of a pay-per-use gateway. - Added the API for querying constraints of a gateway. - Added the API for querying quotas of a credential. - Added the API for configuring access control settings of an app. - Added the API for querying access control details of an app. - Added the API for deleting access control settings of an app. - Added credential quota management APIs.
2022-12-13	- Added the API for querying tags of all gateways in a project. - Added the API for querying tags of a gateway. - Added the API for adding or deleting tags of a gateway.
2022-12-02	- Added the API for enabling backend servers. - Added the API for disabling backend servers. - Added the API for modifying VPC channel health checks. - Added the API for adding or updating a backend server group of a VPC channel. - Added the API for querying backend server groups of a VPC channel. - Added the API for viewing details about a backend server group of a VPC channel. - Added the API for deleting a backend server group of a VPC channel. - Added the API for updating a backend server group of a VPC channel.
2022-11-16	Added descriptions about plug-in management APIs.
2022-11-01	Added descriptions about microservice center management APIs.
2022-11-09	Added descriptions about SSL certificate management APIs.
2021-06-15	Added dedicated gateway APIs.

Released On	Change History
2019-03-08	Added descriptions about domain name management APIs.
2018-11-19	This issue is the first official release.