API Gateway

Service Notice

Issue	01
Date	2024-12-02

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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.

Contents

1 Product Bulletin

1.1 Action Change Notice

Description

From September 2024, if users use custom policies to access the following APIs, they need to create new or update existing custom policies.

Permission	API	New Action	Related Action	IAM Project	Enterprise Project
Querying SSL Certificates	GET /v2/{project_id}/apigw/certificates	apig:certificate:list	-	√	√

Permission	API	New Action	Related Action	IAM Project	Enterprise Project
Adding an SSL certificate	POST /v2/{project_id}/apigw/certificates	apig:certificate:create	apig:instances:get	√	Supported only when the parameter **instance_id** is carried in the request.
Deleting an SSL certificate	DELETE /v2/{project_id}/apigw/certificates/{certificate_id}	apig:certificate:delete	-	√	×
Querying Certificate Details	GET /v2/{project_id}/apigw/certificates/{certificate_id}	apig:certificate:get	-	√	×

Permission	API	New Action	Related Action	IAM Project	Enterprise Project
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	-	√	×
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	√	×
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	√	×
Querying VPC Endpoint Connections	GET /v2/{project_id}/apigw/instances/{instance_id}/vpc-endpoint/connections	apig:instance:listVpcEndpoint	apig:instances:get	√	√

Permission	API	New Action	Related Action	IAM Project	Enterprise Project
Accepting or Rejecting a VPC Endpoint Connection	POST /v2/{project_id}/apigw/instances/{instance_id}/vpc-endpoint/connections/action	apig:instance:acceptOrRejectVpcEndpointConnection	apig:instances:get	√	√
Querying Whitelist Records of a VPC Endpoint Service	GET /v2/{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions	apig:instance:listVpcEndpointPermission	apig:instances:get	√	√
Adding Whitelist Records for a VPC Endpoint Service	POST/v2/{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions/batch-add	apig:instance:batchAddVpcEndpointPermission	apig:instances:get	√	√
Deleting Whitelist Records of a VPC Endpoint Service	POST/v2/{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions/batch-delete	apig:instance:batchDeleteVpcEndpointPermission	apig:instances:get	√	√
Creating a Parameter Orchestration Rule	POST /v2/{project_id}/apigw/instances/{instance_id}/orchestration	apig:orchestration:create	apig:instances:get	√	√
Viewing Orchestration Rules	GET /v2/{project_id}/apigw/instances/{instance_id}/orchestration	apig:orchestration:list	apig:instances:get	√	√
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	√	√

Permission	API	New Action	Related Action	IAM Project	Enterprise Project
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	√	√

Scope

All regions

Impact

If a custom policy does not contain the preceding actions, users assigned this policy cannot access these APIs.

Solution

Create or update custom policies, add the preceding new actions and related actions, and assign custom policies to user groups for fine-grained access control. For details about custom policies, see **APIG Custom Policies**.

2 Vulnerability Notices

2.1 Vulnerability Fixing Policies

APIG Vulnerability Fixing Time

- SDK vulnerabilities:

  For a vulnerability involved in the SDKs provided by APIG, a fix will be provided in line with the risk level within the fixing time. You can fix the vulnerability on your own.

- Other vulnerabilities:

  Upgrade versions to fix other vulnerabilities.

Fixing Statement

To prevent customers from being exposed to unexpected risks, API Gateway (APIG) does not provide other information about the vulnerability except the vulnerability background, details, technical analysis, affected functions/versions/scenarios, solutions, and reference information.

In addition, APIG provides the same information for all customers to protect all customers equally. APIG will not notify individual customers in advance.

APIG does not develop or release intrusive code (or code for verification) to exploit vulnerabilities.

