

Web Application Firewall

Referencia de la API

Edición 01
Fecha 2022-11-01



Copyright © Huawei Technologies Co., Ltd. 2022. Todos los derechos reservados.

Quedan terminantemente prohibidas la reproducción y la divulgación del presente documento en todo o en parte, de cualquier forma y por cualquier medio, sin la autorización previa de Huawei Technologies Co., Ltd. otorgada por escrito.

Marcas y permisos



HUAWEI y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.

Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

Huawei Technologies Co., Ltd.

Dirección: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Sitio web: <https://www.huawei.com>

Email: support@huawei.com

Índice

1 Antes de empezar.....	1
1.1 Descripción general.....	1
1.2 Llamadas a la API.....	1
1.3 Conceptos.....	1
2 Descripción general de API.....	3
3 Llamadas a la API.....	4
3.1 Realización de una solicitud de API.....	4
3.2 Autenticación.....	7
3.3 Respuesta.....	8
4 API.....	10
4.1 Gestión de sitios web protegidos en modo Cloud.....	10
4.1.1 Consultar la lista de nombres de dominio protegidos con Cloud WAF.....	10
4.1.2 Adición de un nombre de dominio a la nube WAF.....	15
4.1.3 Cambio del estado de protección de un nombre de dominio.....	21
4.1.4 Obtención de información de enrutamiento de nombres de dominio (en modo Cloud).....	25
4.1.5 Consulta de un nombre de dominio por ID en modo de cloud.....	28
4.1.6 Actualización de nombres de dominio protegidos con la nube WAF.....	32
4.1.7 Eliminación de un nombre de dominio de la Cloud WAF.....	41
4.2 Gestión de políticas.....	46
4.2.1 Consulta de una lista de política.....	46
4.2.2 Creación de una política de protección.....	52
4.2.3 Consulta de una política por ID.....	59
4.2.4 Actualización de una política de protección aplicada a un nombre de dominio.....	65
4.2.5 Actualización de una política de protección.....	72
4.2.6 Eliminación de una política.....	82
4.3 Gestión de reglas.....	88
4.3.1 Eliminación de una regla de enmascaramiento de falsa alarma.....	88
4.3.2 Consulta de la lista de reglas de enmascaramiento de falsa alarma.....	93
4.3.3 Adición de una regla de enmascaramiento de falsa alarma.....	98
4.3.4 Consulta de la lista de tablas de referencia.....	104
4.3.5 Creación de una tabla de referencia.....	107
4.3.6 Modificación de una tabla de referencia.....	111

4.3.7 Eliminación de una tabla de referencia.....	114
4.3.8 Cambio del estado de una regla.....	117
4.3.9 Consulta de la lista de reglas de la lista negra y la lista blanca.....	120
4.3.10 Creación de una regla de lista negra/lista blanca.....	124
4.3.11 Actualización de una regla de protección de listas negras o blancas.....	127
4.3.12 Eliminación de una regla de lista negra o de lista blanca.....	130
4.3.13 Creación de una regla de enmascaramiento de datos.....	133
4.3.14 Consulta de una regla de enmascaramiento de datos.....	137
4.3.15 Actualización de una regla de enmascaramiento de datos.....	140
4.3.16 Eliminación de una regla de enmascaramiento de datos.....	144
4.3.17 Consulta de la lista de reglas de control de acceso de geolocalización.....	147
4.3.18 Creación de una regla de control de acceso de geolocalización.....	151
4.3.19 Actualización de una regla de control de acceso de geolocalización.....	155
4.3.20 Eliminación de una regla de control de acceso de geolocalización.....	160
4.3.21 Consulta de la lista de reglas de protección web contra manipulaciones.....	164
4.3.22 Creación de una regla de protección contra manipulaciones Web.....	167
4.3.23 Eliminación de una regla de protección contra manipulaciones web.....	170
4.4 Certificate Management.....	173
4.4.1 Aplicación de un certificado a un nombre de dominio.....	173
4.4.2 Consulta de la lista de certificados.....	176
4.4.3 Creación de un certificado.....	180
4.4.4 Consulta de un certificado.....	184
4.4.5 Eliminación de un certificado.....	188
4.4.6 Modificación de un certificado.....	191
4.5 Gestión de Eventos.....	194
4.5.1 Esta API se utiliza para consultar la lista de eventos de ataque.....	194
4.5.2 Esta API se utiliza para consultar detalles de eventos de ataque.....	199
4.6 Panel de control.....	203
4.6.1 Consulta de estadísticas de solicitud de sitio web.....	203
4.6.2 Consulta de las estadísticas de QPS.....	206
4.6.3 Consulta de estadísticas de uso de ancho de banda.....	210
4.6.4 Consulta del número de solicitudes anormales.....	213
4.7 Consulta de características disponibles en un sitio.....	216
4.7.1 Consulta de características disponibles en un sitio.....	217
4.8 Consulta de los nombres de dominio de una cuenta.....	220
4.8.1 Consulta de la lista de nombres de dominio protegidos.....	220
4.9 Consulta de un nombre de dominio de una cuenta.....	225
4.9.1 Consultar un nombre de dominio por ID.....	225
4.10 Gestión de sitios web protegidos en modo dedicado.....	229
4.10.1 Adición de un nombre de dominio a una instancia WAF dedicada.....	229
4.10.2 Consulta de nombres de dominio protegidos por motores WAF dedicados.....	234
4.10.3 Modificación de un nombre de dominio protegido por una instancia WAF dedicada.....	238

4.10.4 Configuración de consultas de nombres de dominio protegidos con instancias WAF dedicadas.....	246
4.10.5 Eliminación de un nombre de dominio de una instancia WAF dedicada.....	253
4.10.6 Modificación del estado de protección de un nombre de dominio en modo dedicado.....	257
A Apéndice.....	261
A.1 Código de estado.....	261
A.2 Códigos de error.....	262
A.3 Obtención de un ID de proyecto.....	266

1 Antes de empezar

1.1 Descripción general

Web Application Firewall (WAF) mantiene los servicios web estables y seguros. Examina todas las solicitudes HTTP y HTTPS para detectar y bloquear los siguientes ataques: inyección de lenguaje de consulta estructurado (SQL), secuencias de comandos en sitios cruzados (XSS), shells web, inyecciones de comandos y código, inclusión de archivos, acceso a archivos confidenciales, vulnerabilidades de terceros, ataque Challenge Collapsar (CC), rastreadores maliciosos y falsificación de solicitudes entre sitios (CSRF).

Este documento describe cómo utilizar las interfaces de programación de aplicaciones (API) para realizar operaciones en WAF, como consultas y actualizaciones.

Antes de comenzar, asegúrese de que está familiarizado con WAF. Para obtener más información, consulte [Web Application Firewall \(WAF\)](#).

1.2 Llamadas a la API

WAF proporciona APIs de Transferencia de Estado Representacional (REST), lo que le permite usar solicitudes HTTPS para llamarlas. Para más detalles, consulte [Llamadas a la API](#).

1.3 Conceptos

- Cuenta
Una cuenta se crea tras el registro exitoso. La cuenta tiene permisos de acceso completos para todos sus servicios y recursos en la nube. Se puede utilizar para restablecer contraseñas de usuario y conceder permisos de usuario. La cuenta es una entidad de pago y no debe usarse para realizar una gestión rutinaria. Por motivos de seguridad, cree usuarios de IAM y concédeles permisos para la gestión rutinaria.
- Usuario
Un usuario de IAM es creado por una cuenta en IAM para usar servicios en la nube. Cada usuario de IAM tiene sus propias credenciales de identidad (contraseña y claves de acceso).

- Región

Las regiones se dividen en función de la ubicación geográfica y la latencia de la red. Los servicios públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) y Image Management Service (IMS), se comparten dentro de la misma región. Las regiones se clasifican como regiones universales y regiones dedicadas. Una región universal proporciona servicios en la nube universales para inquilinos comunes. Una región dedicada proporciona servicios del mismo tipo solo o para inquilinos específicos.

2 Descripción general de API

Puede utilizar todas las funciones de WAF a través de sus APIs.

Tipo	Descripción
Cloud mode APIs	API para crear, modificar, consultar y eliminar nombres de dominio en modo nube.
Dedicated mode APIs	API para crear, modificar, consultar y eliminar nombres de dominio en modo dedicado
Certificate APIs	API para crear, modificar y consultar certificados.
Protection rule APIs	API para crear, actualizar, consultar y eliminar reglas de protección.
Protection policy APIs	API para crear políticas en lotes y modificar los nombres de dominio a los que se aplica una política.
Event API	API para consultar detalles de un evento.
Domain name query API	API para consultar nombres de dominio conectados a WAF

3 Llamadas a la API

3.1 Realización de una solicitud de API

Esta sección describe la estructura de una solicitud de API de REST y utiliza la API de IAM para **obtener un token de usuario** como ejemplo para demostrar cómo llamar a una API. El token obtenido se puede usar entonces para autenticar la llamada de otras API.

Solicitud de URI

Un URI de solicitud tiene el siguiente formato:

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

Aunque se incluye un URI de solicitud en la cabecera de solicitud, la mayoría de los lenguajes de programación o marcos requieren que el URI de solicitud se transmita por separado.

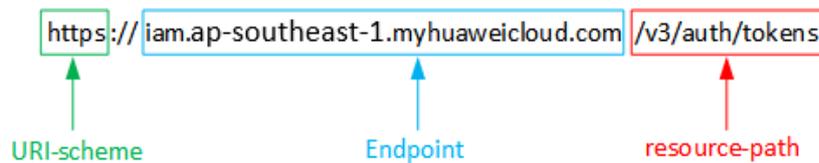
- **URI-scheme:**
Protocolo utilizado para transmitir solicitudes. Todas las API usan HTTPS.
- **Endpoint:**
Nombre de dominio o dirección IP del servidor que lleva el servicio REST. El endpoint varía entre los servicios en diferentes regiones. Se puede obtener del [Regiones y endpoints](#).
Por ejemplo, el endpoint de IAM en la región **CN-Hong Kong** es iam.ap-southeast-1.myhuaweicloud.com.
- **resource-path:**
Ruta de acceso de una API para realizar una operación especificada. Obtenga la ruta de acceso desde el URI de una API. Por ejemplo, **resource-path** de la API utilizada para obtener un token de usuario es **/v3/auth/tokens**.
- **query-string:**
Parámetro de consulta, que es opcional. Asegúrese de que se incluya un signo de interrogación (?) antes de cada parámetro de consulta que tenga el formato de "Nombre de parámetro=Valor de parámetro". Por ejemplo, **?limit=10** indica que se mostrará un máximo de 10 registros de datos.

Por ejemplo, para obtener un token IAM en la región **CN-Hong Kong**, obtener el endpoint de IAM (iam.ap-southeast-1.myhuaweicloud.com) para esta región y **resource-path** (**/v3/auth/**

tokens) en el URI de la API utilizada para **obtener un token de usuario**. A continuación, construya el URI de la siguiente manera:

```
https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
```

Figura 3-1 URI de ejemplo



📖 NOTA

Para simplificar la visualización de URI en este documento, cada API se proporciona solo con **resource-path** y un método de solicitud. El **URI-scheme** de todas las API es **HTTPS**, y los endpoints de todas las API de la misma región son idénticos.

Métodos de solicitud

El protocolo HTTP define los siguientes métodos de solicitud que se pueden usar para enviar una solicitud al servidor:

- **GET**: solicita al servidor que devuelva los recursos especificados.
- **PUT**: solicita al servidor que actualice los recursos especificados.
- **POST**: solicita al servidor que añada recursos o realice operaciones especiales.
- **DELETE**: solicita al servidor que elimine los recursos especificados, por ejemplo, un objeto.
- **HEAD**: igual que GET excepto que el servidor debe devolver solo el encabezado de respuesta.
- **PATCH**: solicita al servidor que actualice el contenido parcial de un recurso especificado. Si el recurso no existe, se creará un nuevo recurso.

Por ejemplo, en el caso de la API usada para **obtener un token de usuario**, el método de solicitud es POST. La solicitud es la siguiente:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
```

Encabezado de la solicitud

También puede agregar campos de encabezado adicionales a una solicitud, como los campos requeridos por un método URI o HTTP especificado. Por ejemplo, para solicitar la información de autenticación, agregue **Content-Type**, que especifica el tipo de cuerpo de la solicitud.

Los campos de encabezado de solicitud comunes son los siguientes:

- **Content-Type**: especifica el tipo o formato del cuerpo de la solicitud. Este campo es obligatorio y su valor predeterminado es **application/json**. Otros valores de este campo se proporcionarán para APIs específicas si los hay.
- **X-Auth-Token**: especifica un token de usuario solo para la autenticación API basada en tokens. El token de usuario es una respuesta a la API utilizada para **obtener un token de usuario**. Esta API es la única que no requiere autenticación.

NOTA

Además de admitir la autenticación basada en tokens, las API también admiten la autenticación mediante ID de clave de acceso/clave de acceso secreta (AK/SK). Durante la autenticación basada en AK/SK, se utiliza un SDK para firmar la solicitud, y los campos de encabezado **Authorization** (información de firma) y **X-Sdk-Date** (hora en la que se envía la solicitud) se añaden automáticamente a la solicitud.

Para obtener más información, consulte [Autenticación basada en AK/SK](#).

La API usada para [obtener un token de usuario](#) no requiere autenticación. Por lo tanto, solo es necesario agregar el campo Content-Type a las solicitudes para llamar a la API. Un ejemplo de tales solicitudes es el siguiente:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
```

Cuerpo de la solicitud

El cuerpo de una solicitud se envía a menudo en un formato estructurado como se especifica en el campo de encabezado Content-Type. El cuerpo de la solicitud transfiere contenido excepto el encabezado de la solicitud.

El cuerpo de la solicitud varía entre las API. Algunas API no requieren el cuerpo de la solicitud, como las API solicitadas mediante los métodos GET y DELETE.

En el caso de la API usada para [obtener un token de usuario](#), los parámetros de solicitud y la descripción de parámetros se pueden obtener a partir de la solicitud de API. A continuación se proporciona una solicitud de ejemplo con un cuerpo incluido. Establecer **username** en el nombre de un usuario, **domainname** en el nombre de la cuenta que el usuario pertenece to, ********* a la contraseña de inicio de sesión del usuario, y **xxxxxxxxxxxxxxxxxxxx** al nombre del proyecto. Puede obtener más información sobre los proyectos en [Regiones y endpoint](#). Compruebe el valor de la columna **Region**.

NOTA

El parámetro **scope** especifica dónde surte efecto un token. Puede establecer **scope** para una cuenta o un proyecto en una cuenta. En el siguiente ejemplo, el token solo tiene efecto para los recursos de un proyecto especificado. Para obtener más información sobre esta API, consulte [Obtener un token de usuario](#).

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
```

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

```
}  
  }  
}  
}
```

Si todos los datos necesarios para la solicitud de API están disponibles, puedes enviar la solicitud para llamar a la API a través de [curl](#), [Postman](#) o codificación. En la respuesta a la API utilizada para obtener un token de usuario, **x-subject-token** es el token de usuario deseado. Este token se puede utilizar para autenticar la llamada de otras API.

3.2 Autenticación

Las solicitudes para llamar a una API se pueden autenticar mediante cualquiera de los siguientes métodos:

- Autenticación basada en tokens: las solicitudes se autentican mediante un token.
- Autenticación basada en AK/SK: Las solicitudes se autentican cifrando el cuerpo de la solicitud usando un par AK/SK. Se recomienda este método porque proporciona mayor seguridad que la autenticación basada en tokens.

Autenticación basada en tokens

NOTA

El período de validez de un token es de 24 horas. Cuando utilice un token para la autenticación, guarde en caché para evitar llamar con frecuencia a la API de IAM utilizada para obtener un token de usuario.

Un token especifica los permisos temporales en un sistema informático. Durante la autenticación de API mediante un token, el token se agrega a las solicitudes para obtener permisos para llamar a la API.

El token se puede obtener llamando a la API requerida. Para obtener más información, consulte [Obtener un token de usuario](#). Se requiere un token de nivel de proyecto para llamar a esta API, es decir, **auth.scope** debe configurarse en **project** en el cuerpo de la solicitud. Por ejemplo:

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

Después de obtener un token, el campo de encabezado X-Auth-Token debe agregarse a las solicitudes para especificar el token al llamar a otras API. Por ejemplo, si el token es

ABCDEFJ..., X-Auth-Token: ABCDEFJ... se puede agregar a una solicitud de la siguiente manera:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

Autenticación basada en AK/SK

NOTA

La autenticación basada en AK/SK admite solicitudes de API con un cuerpo de no más de 12 MB. Para las solicitudes de API con un cuerpo más grande, se recomienda la autenticación basada en tokens.

En la autenticación basada en AK/SK, AK/SK se utiliza para firmar solicitudes y la firma se añade a continuación a las solicitudes de autenticación.

- **AK:** ID de clave de acceso, que es un identificador único utilizado junto con una clave de acceso secreta para firmar solicitudes criptográficamente.
- **SK:** clave de acceso secreta usada junto con una AK para firmar solicitudes criptográficamente. Identifica un remitente de la solicitud y evita que la solicitud sea modificada.

En la autenticación basada en AK/SK, puede usar una AK/SK para firmar solicitudes basadas en el algoritmo de firma o usar el SDK de firma para firmar solicitudes. Para obtener más información sobre cómo firmar solicitudes y usar el SDK de firma, consulte [Guía de firma de API](#).

AVISO

El SDK de firma solo se utiliza para firmar solicitudes y es diferente de los SDK proporcionados por los servicios.

3.3 Respuesta

Código de estado

Después de enviar una solicitud, recibirá una respuesta, que incluye un código de estado, un encabezado de respuesta y un cuerpo de respuesta.

Un código de estado es un grupo de dígitos, que van desde 1xx hasta 5xx. Indica el estado de una solicitud. Para obtener más información, consulte [Código de estado](#).

Por ejemplo, si se devuelve el código de estado **201** para llamar a la API utilizada para [obtener un token de usuario](#).

Encabezado de respuesta

Similar a una solicitud, una respuesta también tiene una cabecera, por ejemplo, **Content-Type**.

A continuación se muestra la cabecera de respuesta para que la API [obtenga un token de usuario](#), en el que **x-subject-token** es el token de usuario deseado. Este token se puede utilizar para autenticar la llamada de otras API.

Figura 3-2 Campos de encabezado de la respuesta a la solicitud de obtención de un token de usuario

```

connection → keep-alive

content-type → application/json

date → Tue, 12 Feb 2019 06:52:13 GMT

server → Web Server

strict-transport-security → max-age=31536000; includeSubdomains;

transfer-encoding → chunked

via → proxy A

x-content-type-options → nosniff

x-download-options → noopen

x-frame-options → SAMEORIGIN

x-iam-trace-id → 218d45ab-d674-4995-af3a-2d0255ba41b5

x-subject-token
→ MIIYXQYJKoZIhvcNAQcColIYTjCCGEOCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BwGgghacBIIWmHsidG9rZW4iOnsiZXhwaXJlc19hdCI6IjIwMTktMDItMTNUMD
fj3Kjs6YgKnpVNRbW2eZ5eb78SZOkqjACgklqO1wi4JIGzrpd18LGXK5bdfq4lqHCYb8P4NaY0NYejcAgzJVeFYtLWT1GSO0zxKZmlQHj82HBqHdglZO9fuEbL5dMhdavj+33wEl
xHRCE9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXl1jipPEGA270g1FruooL6jgglFkNPQuFSOU8+uSsttVwRtnfsC+qTp22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUUVhVpxk8pxiX1wTEboX-
RzT6MUbpvGw-oPNFYxjECKnoH3HRozv0vN--n5d6Nbxg==

x-xss-protection → 1; mode=block;
    
```

(Opcional) Cuerpo de respuesta

El cuerpo de una respuesta se devuelve a menudo en formato estructurado como se especifica en el campo de encabezado **Content-Type**. El cuerpo de la respuesta transfiere contenido excepto el encabezado de la respuesta.

A continuación se muestra parte del cuerpo de respuesta para que la API **obtenga un token de usuario**. En aras del espacio, solo una parte del contenido se muestra aquí.

```

{
  "token": {
    "expires_at": "2019-02-13T06:52:13.855000Z",
    "methods": [
      "password"
    ],
    "catalog": [
      {
        "endpoints": [
          {
            "region_id": "xxxxxxxx",
            .....
          }
        ]
      }
    ]
  }
}
    
```

Si se produce un error durante la llamada a la API, se mostrará un código de error y un mensaje. A continuación se muestra un cuerpo de respuesta de error.

```

{
  "error_msg": "The format of message is error",
  "error_code": "AS.0001"
}
    
```

En el cuerpo de la respuesta, **error_code** es un código de error y **error_msg** proporciona información sobre el error.

4 API

4.1 Gestión de sitios web protegidos en modo Cloud

4.1.1 Consultar la lista de nombres de dominio protegidos con Cloud WAF

Función

Esta API se utiliza para consultar la lista de nombres de dominio protegidos con el WAF en la nube.

URI

GET /v1/{project_id}/waf/instance

Tabla 4-1 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-2 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetro	Obligatorio	Tipo	Descripción
page	No	Integer	Número de página de los datos a devolver durante la consulta de paginación. El valor varía de 0 a 100000 . El valor predeterminado es 1 , que indica que se devuelven los datos de la primera página. Predeterminado: 1
pagesize	No	Integer	Número de resultados en cada página durante la consulta de paginación. El valor varía de 1 a 100 . El valor predeterminado es 10 , lo que indica que cada página contiene 10 resultados. Predeterminado: 10
hostname	No	String	Nombre de dominio
policyname	No	String	Nombre de la política

Parámetros de solicitud

Tabla 4-3 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-4 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Número de nombres de dominio protegidos con la instancia WAF en la nube

Parámetro	Tipo	Descripción
items	Array of CloudWafHostItem objects	Detalles sobre el nombre de dominio protegido

Tabla 4-5 CloudWafHostItem

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostid	String	ID de nombre de dominio
description	String	Descripción.
type	Integer	Modo de implementación WAF
proxy	Boolean	Si el proxy está habilitado
flag	Flag object	Certificaciones soportadas por WAF
hostname	String	Nombre de dominio agregado a la nube WAF.
access_code	String	Prefijo de CNAME
policyid	String	ID de política
timestamp	Long	Hora en que se agrega un nombre de dominio a WAF.
protect_status	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.
access_status	Integer	Estado de acceso
exclusive_ip	Boolean	Si se utiliza una dirección IP dedicada
paid_type	String	Forma de pago. Actualmente, solo se admite el método de prepago. Valores de enumeración: ● prePaid

Tabla 4-6 Flag

Parámetro	Tipo	Descripción
pci_3ds	String	true : Se aprueba la certificación estándar PCI 3DS. false : no se aprueba la certificación estándar PCI 3DS. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
pci_dss	String	true : Se aprueba la certificación estándar PCI DSS. false : no se aprueba la certificación estándar PCI DSS. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
cname	String	old : Se utiliza el antiguo registro CNAME. new : se utiliza un nuevo registro CNAME. Valores de enumeración: <ul style="list-style-type: none"> ● old ● new
is_dual_az	String	true : WAF soporta multi-AZ DR. false : WAF no admite DR multi-AZ. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false

Código de estado: 400

Tabla 4-7 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-8 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error

Parámetro	Tipo	Descripción
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-9 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/instance?enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "d0a4bc2f74e3407388a50243af700305",
    "hostid" : "d0a4bc2f74e3407388a50243af700305",
    "description" : "e",
    "type" : 1,
    "proxy" : false,
    "flag" : {
      "pci_3ds" : "false",
      "pci_dss" : "false",
      "ipv6" : "false",
      "cname" : "new",
      "is_dual_az" : "true"
    },
    "region" : "cn-north-7",
    "hostname" : "www.demo.com",
    "access_code" : "7d06456ffaxxxxxxxxxxxx281bc13b",
    "policyid" : "bb2124fabe6f42ff9fe4770eecb2670",
    "timestamp" : 1642648030687,
    "protect_status" : 1,
    "access_status" : 0,
    "exclusive_ip" : false,
    "web_tag" : "iii",
    "paid_type" : "prePaid"
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.1.2 Adición de un nombre de dominio a la nube WAF

Función

Esta API se utiliza para agregar un nombre de dominio a la nube WAF.

URI

POST /v1/{project_id}/waf/instance

Tabla 4-10 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-11 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API <code>ListEnterpriseProject</code> de EPS.

Parámetros de solicitud

Tabla 4-12 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-13 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
hostname	Sí	String	El nombre de dominio puede contener un máximo de 64 caracteres. Solo se permiten letras, dígitos, guiones (-) guiones bajos y puntos, por ejemplo, www.domain.com.
policyid	No	String	ID de la política utilizada inicialmente para el nombre de dominio. Se puede obtener llamando a la API ListPolicy .
server	Sí	Array of CloudWafServer objects	Detalles del servidor de origen
certificateid	No	String	ID del certificado. Se puede obtener llamando a la API de ListCertificates . \n - Este parámetro no es necesario cuando el protocolo cliente es HTTP. \n - Este parámetro es obligatorio cuando el protocolo cliente es HTTPS.
certificatename	No	String	Nombre del certificado. \n - Este parámetro no es necesario cuando el protocolo cliente es HTTP. \n - Este parámetro es obligatorio cuando el protocolo cliente es HTTPS.
proxy	Sí	Boolean	Si se utiliza un proxy para el nombre de dominio

Parámetro	Obligatorio	Tipo	Descripción
description	No	String	Descripción del nombre de dominio

Tabla 4-14 CloudWafServer

Parámetro	Obligatorio	Tipo	Descripción
front_protocol	Sí	String	Protocolo del cliente Valores de enumeración: ● HTTP ● HTTPS
back_protocol	Sí	String	Protocolo de servidor Valores de enumeración: ● HTTP ● HTTPS
address	Sí	String	Dirección del servidor
port	Sí	Integer	Puerto del servidor
type	Sí	String	La dirección del servidor de origen es una dirección IPv4 o IPv6. Valores de enumeración: ● ipv4 ● ipv6

Parámetros de respuesta

Código de estado: 200

Tabla 4-15 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio agregado a la nube WAF.
policyid	String	ID de política
access_code	String	Prefijo de CNAME

Parámetro	Tipo	Descripción
protect_status	Integer	Estado de protección del nombre de dominio. \n - 1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.
access_status	Integer	Estado de acceso
protocol	String	Tipo de protocolo de cliente devuelto
certificateid	String	ID de certificado devuelto
certificatename	String	Nombre del certificado
server	Array of CloudWafServer objects	Detalles del servidor de origen
flag	Flag object	Certificaciones soportadas por WAF
proxy	Boolean	Si el proxy está habilitado
timestamp	Long	Hora en que se agrega un nombre de dominio a WAF.
exclusive_ip	Boolean	Si se utiliza una dirección IP dedicada
http2_enable	Boolean	Compatibilidad con HTTP/2

Tabla 4-16 CloudWafServer

Parámetro	Tipo	Descripción
front_protocol	String	Protocolo del cliente Valores de enumeración: <ul style="list-style-type: none"> ● HTTP ● HTTPS
back_protocol	String	Protocolo de servidor Valores de enumeración: <ul style="list-style-type: none"> ● HTTP ● HTTPS
address	String	Dirección del servidor
port	Integer	Puerto del servidor

Parámetro	Tipo	Descripción
type	String	La dirección del servidor de origen es una dirección IPv4 o IPv6. Valores de enumeración: <ul style="list-style-type: none"> ● ipv4 ● ipv6

Tabla 4-17 Flag

Parámetro	Tipo	Descripción
pci_3ds	String	true : Se aprueba la certificación estándar PCI 3DS. false : no se aprueba la certificación estándar PCI 3DS. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
pci_dss	String	true : Se aprueba la certificación estándar PCI DSS. false : no se aprueba la certificación estándar PCI DSS. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
cname	String	old : Se utiliza el antiguo registro CNAME. new : se utiliza un nuevo registro CNAME. Valores de enumeración: <ul style="list-style-type: none"> ● old ● new
is_dual_az	String	true : WAF soporta multi-AZ DR. false : WAF no admite DR multi-AZ. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false

Código de estado: 400

Tabla 4-18 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error

Parámetro	Tipo	Descripción
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-19 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-20 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
POST https://{Endpoint}/v1/{project_id}/waf/instance?enterprise_project_id=0
{
  "hostname" : "www.demo.com",
  "server" : [ {
    "front_protocol" : "HTTPS",
    "back_protocol" : "HTTP",
    "type" : "ipv4",
    "address" : "x.x.x.x",
    "port" : "7443"
  } ],
  "proxy" : false,
  "paid_type" : "prePaid",
  "description" : "demo",
  "web_tag" : "demo",
  "certificateid" : "3ac1402300374a63a05be68c641e92c8",
  "certificatename" : "test6",
  "exclusive_ip" : false
}
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "31af669f567246c289771694f2112289",
```

```

"hostname" : "www.demo.com",
"protocol" : "HTTP",
"server" : [ {
  "address" : "x.x.x.x",
  "port" : 80,
  "type" : "ipv4",
  "http2" : false,
  "weight" : 1,
  "front_protocol" : "HTTP",
  "back_protocol" : "HTTP"
} ],
"proxy" : false,
"locked" : 0,
"timestamp" : 1650527546420,
"flag" : {
  "pci_3ds" : "false",
  "pci_dss" : "false",
  "ipv6" : "false",
  "cname" : "new",
  "is_dual_az" : "true"
},
"description" : "",
"policyid" : "41cba8aee2e94bcdbf57460874205494",
"domainid" : "d4ecb00b031941ce9171b7bc3386883f",
"projectid" : "0456cf04d6f64725ab02ed5bd2efd44",
"enterprise_project_id" : "0",
"protect_status" : 1,
"access_status" : 0,
"access_code" : "1b18879b9d064f8bbcbf8abce7294cac",
"block_page" : {
  "template" : "default"
},
"web_tag" : "",
"exclusive_ip" : false,
"http2_enable" : false
}

```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.1.3 Cambio del estado de protección de un nombre de dominio

Función

información de enrutamiento

URI

PUT /v1/{project_id}/waf/instance/{instance_id}/protect-status

Tabla 4-21 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
instance_id	Sí	String	ID de nombre de dominio. Se puede obtener llamando a la API ListHost .

Tabla 4-22 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-23 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-24 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
protect_status	Sí	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.

Parámetros de respuesta

Código de estado: 200

Tabla 4-25 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
protect_status	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.

Código de estado: 400

Tabla 4-26 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-27 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-28 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
POST https://{Endpoint}/v1/{project_id}/waf/instance/{instance_id}/protect-status?
enterprise_project_id=0

{
  "protect_status" : 0
}
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "protect_status" : 0
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.1.4 Obtención de información de enrutamiento de nombres de dominio (en modo Cloud)

Función

información de enrutamiento

URI

GET /v1/{project_id}/waf/instance/{instance_id}/route

Tabla 4-29 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
instance_id	Sí	String	ID de nombre de dominio. Se puede obtener llamando a la API ListHost .

Tabla 4-30 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-31 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-32 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Cantidad
items	Array of RouteBody objects	Cuerpo de ruta.

Tabla 4-33 RouteBody

Parámetro	Tipo	Descripción
cname	String	Sufijo CNAME
name	String	Nombre
servers	Array of RouteServerBody objects	Información de la ruta

Tabla 4-34 RouteServerBody

Parámetro	Tipo	Descripción
back_protocol	String	Protocolo
address	String	Dirección IP del servidor backend
port	Integer	Puerto

Código de estado: 400

Tabla 4-35 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-36 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-37 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/instance/{instance_id}/route?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "total" : 1,
  "items" : [ {
    "cname" : "e9d30fda6xxxxxxxxxxxxx5b3d3286",
    "name" : "Beijing",
    "servers" : [ {
      "back_protocol" : "HTTP",
      "address" : "x.x.x.x",
      "port" : 80
    } ]
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.1.5 Consulta de un nombre de dominio por ID en modo de cloud

Función

Consulta de un nombre de dominio por ID en modo cloud

URI

GET /v1/{project_id}/waf/instance/{instance_id}

Tabla 4-38 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
instance_id	Sí	String	ID de nombre de dominio. Se puede obtener llamando a la API ListHost para la nube WAF.

Tabla 4-39 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-40 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-41 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio agregado a la nube WAF.
policyid	String	ID de política
access_code	String	Prefijo de CNAME
protect_status	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.
access_status	Integer	Estado de acceso
protocol	String	Tipo de protocolo de backend. El valor puede ser HTTPS, HTTP o HTTP&HTTPS.
certificateid	String	ID de certificado HTTPS.
certificatename	String	Nombre del certificado
server	Array of CloudWafServer objects	Detalles del servidor de origen
proxy	Boolean	Si el proxy está habilitado.
timestamp	Long	Hora en que se agrega un nombre de dominio a WAF.
exclusive_ip	Boolean	Si se utiliza una dirección IP dedicada

Tabla 4-42 CloudWafServer

Parámetro	Tipo	Descripción
front_protocol	String	Protocolo del cliente Valores de enumeración: ● HTTP ● HTTPS

Parámetro	Tipo	Descripción
back_protocol	String	Protocolo de servidor Valores de enumeración: <ul style="list-style-type: none"> ● HTTP ● HTTPS
address	String	Dirección del servidor
port	Integer	Puerto del servidor
type	String	La dirección del servidor de origen es una dirección IPv4 o IPv6. Valores de enumeración: <ul style="list-style-type: none"> ● ipv4 ● ipv6

Código de estado: 400

Tabla 4-43 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-44 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-45 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/instance/{instance_id}?  
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{  
  "id" : "31af669f567246c289771694f2112289",  
  "hostname" : "www.demo.com",  
  "protocol" : "HTTP",  
  "server" : [ {  
    "address" : "x.x.x.x",  
    "port" : 80,  
    "type" : "ipv4",  
    "http2" : false,  
    "weight" : 1,  
    "front_protocol" : "HTTP",  
    "back_protocol" : "HTTP"  
  } ],  
  "proxy" : false,  
  "locked" : 0,  
  "timestamp" : 1650527546420,  
  "flag" : {  
    "pci_3ds" : "false",  
    "pci_dss" : "false",  
    "ipv6" : "false",  
    "cname" : "new",  
    "is_dual_az" : "true"  
  },  
  "description" : "",  
  "policyid" : "41cba8aee2e94bcdbf57460874205494",  
  "domainid" : "d4ecb00b031941ce9171b7bc3386883f",  
  "projectid" : "0456cf04d6f64725ab02ed5bd2efdfa4",  
  "enterprise_project_id" : "0",  
  "protect_status" : 0,  
  "access_status" : 0,  
  "access_code" : "1b18879b9d064f8bbcbf8abce7294cac",  
  "block_page" : {  
    "template" : "default"  
  },  
  "web_tag" : "",  
  "exclusive_ip" : false,  
  "http2_enable" : false  
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.1.6 Actualización de nombres de dominio protegidos con la nube WAF

Función

Esta API se utiliza para actualizar los nombres de dominio protegidos con el WAF en la nube. La nueva información del servidor de origen sobrescribirá la información del servidor de origen antiguo. Si desea conservar la información antigua, indíquela como datos nuevos.

URI

PATCH /v1/{project_id}/waf/instance/{instance_id}

Tabla 4-46 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
instance_id	Sí	String	ID de nombre de dominio. Se puede obtener llamando a la API ListHost .

Tabla 4-47 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-48 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).

Parámetro	Obligatorio	Tipo	Descripción
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-49 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
proxy	No	Boolean	Si se utiliza un proxy para el nombre de dominio
certificateid	No	String	ID del certificado. Este parámetro está disponible cuando se utiliza HTTPS para el protocolo de cliente. Se puede obtener llamando a la API de ListCertificates .
certificatename	No	String	Nombre del certificado. Este parámetro está disponible cuando se utiliza HTTPS para el protocolo de cliente. Se puede obtener llamando a la API de ListCertificates . También puede ir a la consola para consultar el nombre del certificado.
server	No	Array of UpdateCloudWafServer objects	Configuración del servidor
tls	No	String	Versión mínima de TLS soportada. El valor puede ser TLS v1.0, TLS v1.1 o TLS v1.2. TLS v1.0 se utiliza de forma predeterminada. Valores de enumeración: <ul style="list-style-type: none"> ● TLS v1.0 ● TLS v1.1 ● TLS v1.2 ● TLS v1.3

Parámetro	Obligatorio	Tipo	Descripción
cipher	No	String	<p>Conjunto de cifrado. El valor puede ser cipher_1, cipher_2, cipher_3, cipher_4, or cipher_default: \n cipher_1: Los algoritmos criptográficos son ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH. \n cipher_2: Los algoritmos criptográficos son EECDH+AESGCM:EDH+AESGCM. \n cipher_3: The cryptographic algorithms are ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH. \n cipher_4: Los algoritmos criptográficos son ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH. \n cipher_default: Los algoritmos criptográficos son ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM.</p> <p>Valores de enumeración:</p> <ul style="list-style-type: none"> ● cipher_1 ● cipher_2 ● cipher_3 ● cipher_4 ● cipher_default

Tabla 4-50 UpdateCloudWafServer

Parameter	Mandatory	Type	Description
front_protocol	No	String	Protocolo del cliente Valores de enumeración: ● HTTP ● HTTPS
back_protocol	No	String	Protocolo de servidor Valores de enumeración: ● HTTP ● HTTPS
address	No	String	Dirección del servidor
port	No	Integer	Puerto del servidor
type	No	String	La dirección del servidor de origen es una dirección IPv4 o IPv6. Valores de enumeración: ● ipv4 ● ipv6

Parámetros de respuesta

Código de estado: 200

Tabla 4-51 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
policyid	String	ID de política
hostname	String	Nombre de dominio conectado a una instancia WAF en la nube
domainid	String	ID de la cuenta.
access_code	String	Prefijo de CNAME
protocol	String	Tipo de protocolo de backend Valores de enumeración: ● HTTPS ● HTTP ● HTTP&HTTPS

Parámetro	Tipo	Descripción
server	Array of CloudWafServer objects	Detalles del servidor de origen
certificateid	String	ID de certificado HTTPS. Se puede obtener llamando a la API de ListCertificates .
certificatename	String	Nombre del certificado. Se puede obtener llamando a la API de ListCertificates .
proxy	Boolean	Si el proxy está habilitado
locked	Integer	Estado de bloqueo. El valor predeterminado es 0 .
protect_status	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.
access_status	Integer	Estado de acceso
timestamp	Long	Hora en que se agrega un nombre de dominio a WAF.
tls	String	Versión SSL Valores de enumeración: <ul style="list-style-type: none"> ● TLS v1.0 ● TLS v1.1 ● TLS v1.2 ● TLS v1.3

Parámetro	Tipo	Descripción
cipher	String	<p>Conjunto de cifrado. El valor puede ser cipher_1, cipher_2, cipher_3, cipher_4, or cipher_default: \n cipher_1: Los algoritmos criptográficos son ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH. \n cipher_2: Los algoritmos criptográficos son ECDH+AESGCM:EDH+AESGCM. \n cipher_3: The cryptographic algorithms are ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH. \n cipher_4: Los algoritmos criptográficos son ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH. \n cipher_default: Los algoritmos criptográficos son ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM.</p> <p>Valores de enumeración:</p> <ul style="list-style-type: none"> ● cipher_1 ● cipher_2 ● cipher_3 ● cipher_4 ● cipher_default
enterprise_project_id	String	ID del proyecto empresarial
block_page	BlockPage object	Página de configuración de alarma
web_tag	Boolean	Nombre personalizable para un dominio
flag	Flag object	Certificaciones soportadas por WAF
exclusive_ip	Boolean	Si se utiliza una dirección IP dedicada
description	String	Descripción del nombre de dominio

Tabla 4-52 CloudWafServer

Parámetro	Tipo	Descripción
front_protocol	String	Protocolo del cliente Valores de enumeración: <ul style="list-style-type: none"> ● HTTP ● HTTPS
back_protocol	String	Protocolo de servidor Valores de enumeración: <ul style="list-style-type: none"> ● HTTP ● HTTPS
address	String	Dirección del servidor
port	Integer	Puerto del servidor
type	String	La dirección del servidor de origen es una dirección IPv4 o IPv6. Valores de enumeración: <ul style="list-style-type: none"> ● ipv4 ● ipv6

Tabla 4-53 BlockPage

Parámetro	Tipo	Descripción
template	String	Nombre de la plantilla
custom_page	CustomPage object	Página de alarma personalizada
redirect_url	String	URL de redireccionamiento

Tabla 4-54 CustomPage

Parámetro	Tipo	Descripción
código de estado	String	Status Codes
content_type	String	Tipo de contenido de la página de alarma
content	String	Contenido de la página

Tabla 4-55 Flag

Parameter	Type	Description
pci_3ds	String	true : Se aprueba la certificación estándar PCI 3DS. false : no se aprueba la certificación estándar PCI 3DS. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
pci_dss	String	true : Se aprueba la certificación estándar PCI DSS. false : no se aprueba la certificación estándar PCI DSS. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
cname	String	old : Se utiliza el antiguo registro CNAME. new : se utiliza un nuevo registro CNAME. Valores de enumeración: <ul style="list-style-type: none"> ● old ● new
is_dual_az	String	true : WAF soporta multi-AZ DR. false : WAF no admite DR multi-AZ. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false

Código de estado: 400

Tabla 4-56 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-57 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error

Parámetro	Tipo	Descripción
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-58 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
PATCH https://{Endpoint}/v1/{project_id}/waf/instance/{instance_id}?
enterprise_project_id=0
```

```
{
  "server" : [ {
    "address" : "x.x.x.x",
    "port" : "80",
    "type" : "ipv4",
    "http2" : false,
    "weight" : 1,
    "front_protocol" : "HTTP",
    "back_protocol" : "HTTP"
  }, {
    "front_protocol" : "HTTP",
    "back_protocol" : "HTTP",
    "type" : "ipv4",
    "address" : "x.x.x.x",
    "port" : "80"
  } ],
  "ipv6_enable" : false
}
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "e91ad96e379b4bea84f8fcd3d153370",
  "hostname" : "www.demo.com",
  "protocol" : "HTTP",
  "server" : [ {
    "address" : "x.x.x.x",
    "port" : 80,
    "type" : "ipv4",
    "http2" : false,
    "weight" : 1,
    "front_protocol" : "HTTP",
    "back_protocol" : "HTTP"
  }, {
    "address" : "1.1.1.4",
    "port" : 80,

```

```

    "type" : "ipv4",
    "weight" : 1,
    "front_protocol" : "HTTP",
    "back_protocol" : "HTTP"
  } ],
  "proxy" : false,
  "locked" : 0,
  "timestamp" : 1650423573577,
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false",
    "ipv6" : "false",
    "cname" : "new",
    "is_dual_az" : "true"
  },
  "description" : "",
  "policyid" : "f385eceedf7c4c34a4d1def19eafbe85",
  "domainid" : "d4ecb00b031941ce9171b7bc3386883f",
  "projectid" : "0456cf04d6f64725ab02ed5bd2efdfa4",
  "enterprise_project_id" : "0",
  "protect_status" : 1,
  "access_status" : 0,
  "access_code" : "4f5372610cdc44f7970759fcca138c81",
  "block_page" : {
    "template" : "default"
  },
  "web_tag" : "we",
  "exclusive_ip" : false,
  "http2_enable" : false
}

```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.1.7 Eliminación de un nombre de dominio de la Cloud WAF

Función

Esta API se utiliza para eliminar un nombre de dominio de la nube WAF.

URI

DELETE /v1/{project_id}/waf/instance/{instance_id}

Tabla 4-59 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
instance_id	Sí	String	ID de nombre de dominio. Se puede obtener llamando a la API ListHost .

Tabla 4-60 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-61 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-62 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostid	String	ID de nombre de dominio
description	String	Descripción.

Parámetro	Tipo	Descripción
type	Integer	Modo de implementación WAF. El valor predeterminado es 1. Actualmente, solo se admite el proxy inverso.
proxy	Boolean	Si el proxy está habilitado
flag	Flag object	Certificaciones soportadas por WAF
hostname	String	Nombre de dominio agregado a la nube WAF.
access_code	String	Sufijo CNAME
policyid	String	ID de política
timestamp	Long	Hora en que se agrega un nombre de dominio a WAF.
protect_status	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.
access_status	Integer	Estado de acceso. 0 : Inaccesible. 1 : Accesible.
exclusive_ip	Boolean	Si se utiliza una dirección IP dedicada
paid_type	String	Modo de pago basado en paquetes. Actualmente, solo se admite el método de prepago. Valores de enumeración: ● prePaid

Tabla 4-63 Flag

Parámetro	Tipo	Descripción
pci_3ds	String	true : Se aprueba la certificación estándar PCI 3DS. false : no se aprueba la certificación estándar PCI 3DS. Valores de enumeración: ● true ● false

Parámetro	Tipo	Descripción
pci_dss	String	true : Se aprueba la certificación estándar PCI DSS. false : no se aprueba la certificación estándar PCI DSS. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
cname	String	old : Se utiliza el antiguo registro CNAME. new : se utiliza un nuevo registro CNAME. Valores de enumeración: <ul style="list-style-type: none"> ● old ● new
is_dual_az	String	true : WAF soporta multi-AZ DR. false : WAF no admite DR multi-AZ. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false

Código de estado: 400

Tabla 4-64 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-65 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-66 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
DELETE https://{Endpoint}/v1/{project_id}/waf/instance/{instance_id}?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "e91ad96e379b4bea84f8fcda3d153370",
  "hostid" : "e91ad96e379b4bea84f8fcda3d153370",
  "description" : "",
  "type" : 1,
  "proxy" : true,
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false",
    "ipv6" : "true",
    "cname" : "new",
    "is_dual_az" : "true"
  },
  "region" : "cn-north-4",
  "hostname" : "www.demo.com",
  "access_code" : "4f5372610cdc44f7970759fcca138c81",
  "policyid" : "f385eceedf7c4c34a4d1def19eafbe85",
  "timestamp" : 1650423573650,
  "protect_status" : 1,
  "access_status" : 0,
  "exclusive_ip" : false,
  "web_tag" : "we",
  "paid_type" : "prePaid"
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.2 Gestión de políticas

4.2.1 Consulta de una lista de política

Función

Consulta de una lista de política

URI

GET /v1/{project_id}/waf/policy

Tabla 4-67 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-68 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.
page	No	Integer	Número de página de los datos a devolver durante la consulta de paginación. El valor varía de 0 a 100000 . El valor predeterminado es 1 , que indica que se devuelven los datos de la primera página. Predeterminado: 1
pagesize	No	Integer	Número de resultados en cada página durante la consulta de paginación. El valor varía de 1 a 100 . El valor predeterminado es 10 , lo que indica que cada página contiene 10 resultados. Predeterminado: 10
name	No	String	Nombre

Parámetros de solicitud

Tabla 4-69 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-70 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Número total de políticas
items	Array of PolicyResponse objects	Contenido de la política

Tabla 4-71 PolicyResponse

Parámetro	Tipo	Descripción
id	String	ID de política
name	String	Nombre de la política
action	PolicyAction object	Operación
options	PolicyOption object	Opción
level	Integer	Nivel de protección
full_detection	Boolean	Modo de detección en la regla de protección precisa
bind_host	Array of BindHost objects	Información básica sobre el dominio protegido.
timestamp	Long	Hora en que se crea una política

Parámetro	Tipo	Descripción
extend	Map<String,String>	Campo extendido

Tabla 4-72 PolicyAction

Parámetro	Tipo	Descripción
category	String	Nivel de protección. El valor puede ser log o block . log : WAF solo registra eventos. block : WAF bloquea eventos. Valores de enumeración: <ul style="list-style-type: none"> ● block ● log

Tabla 4-73 PolicyOption

Parámetro	Tipo	Descripción
webattack	Boolean	Si la protección web básica está habilitada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
common	Boolean	Si la comprobación general está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler	Boolean	Si la protección antideslizante está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler_engine	Boolean	Si el motor de búsqueda está habilitado Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler_scanner	Boolean	Si la detección antideslizante está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false

Parámetro	Tipo	Descripción
crawler_script	Boolean	Si el antideslizador JavaScript está activado Valores de enumeración: ● true ● false
crawler_other	Boolean	Si está activada la comprobación de otro rastreador Valores de enumeración: ● true ● false
webshell	Boolean	Si la detección de webshell está habilitada Valores de enumeración: ● true ● false
cc	Boolean	Si las reglas de protección contra ataques de CC están habilitadas Valores de enumeración: ● true ● false
custom	Boolean	Si la protección precisa está habilitada Valores de enumeración: ● true ● false
whiteblackip	Boolean	Si la protección de listas negras y blancas está habilitada. Valores de enumeración: ● true ● false
geoip	Boolean	Si el control de acceso de geolocalización está habilitado Valores de enumeración: ● true ● false
ignore	Boolean	Si el enmascaramiento de falsa alarma está habilitado. Valores de enumeración: ● true ● false

Parámetro	Tipo	Descripción
privacy	Boolean	Si el enmascaramiento de datos está habilitado Valores de enumeración: ● true ● false
antitamper	Boolean	Si la protección contra manipulaciones web está activada Valores de enumeración: ● true ● false
antileakage	Boolean	Si la prevención de fugas de información está activada Valores de enumeración: ● true ● false
bot_enable	Boolean	Si la mitigación de bots está habilitada Valores de enumeración: ● true ● false
modulex_enabled	Boolean	Si la protección contra ataques CC para moduleX está habilitada. Esta función se encuentra en la prueba beta abierta (OBT). Durante la OBT, solo se admite el modo de solo registro. Valores de enumeración: ● true ● false

Tabla 4-74 BindHost

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio
waf_type	String	Modo de nombre de dominio: cloud (modo de cloud) / premium (modo dedicado)
mode	String	Este parámetro es requerido solamente por el modo dedicado.

Código de estado: 400

Tabla 4-75 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-76 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-77 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/policy?enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "total" : 1,
  "items" : [ {
    "id" : "41cba8aee2e94bcdbf57460874205494",
    "name" : "policy_2FHwFOKz",
    "level" : 2,
    "action" : {
      "category" : "log",
      "modulex_category" : "log"
    },
    "options" : {
      "webattack" : true,
      "common" : true,
      "crawler" : true,
      "crawler_engine" : false,
      "crawler_scanner" : true,

```

```

"crawler_script" : false,
"crawler_other" : false,
"webshell" : false,
"cc" : true,
"custom" : true,
"precise" : false,
"whiteblackip" : true,
"geoip" : true,
"ignore" : true,
"privacy" : true,
"antitamper" : true,
"anticrawler" : false,
"antileakage" : false,
"followed_action" : false,
"bot_enable" : true,
"modulex_enabled" : false
},
"hosts" : [ ],
"extend" : { },
"timestamp" : 1650527546218,
"full_detection" : false,
"bind_host" : [ ]
} ]
}

```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.2.2 Creación de una política de protección

Función

Esta API se utiliza para crear una política WAF.

URI

POST /v1/{project_id}/waf/policy

Tabla 4-78 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-79 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-80 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-81 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
name	Sí	String	Nombre de la política. Puede contener solo dígitos, letras y guiones bajos (_) y no puede superar los 64 caracteres.

Parámetros de respuesta

Código de estado: 200

Tabla 4-82 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de política
name	String	Nombre de la política
level	Integer	Nivel de protección
action	PolicyAction object	Operación

Parámetro	Tipo	Descripción
options	PolicyOption object	Opción
full_detection	Boolean	Modo de detección en la regla de protección precisa
hosts	Array of strings	ID del sitio web protegido
bind_host	Array of BindHost objects	Información del sitio web protegido
timestamp	Long	Hora en que se crea una política
extend	Object	Campo extendido

Tabla 4-83 PolicyAction

Parámetro	Tipo	Descripción
category	String	Nivel de protección. El valor puede ser log o block . log : WAF solo registra eventos. block : WAF bloquea eventos. Valores de enumeración: <ul style="list-style-type: none"> ● block ● log

Tabla 4-84 PolicyOption

Parámetro	Tipo	Descripción
webattack	Boolean	Si la protección web básica está habilitada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
common	Boolean	Si la comprobación general está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler	Boolean	Si la protección antideslizante está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false

Parámetro	Tipo	Descripción
crawler_engine	Boolean	Si el motor de búsqueda está habilitado Valores de enumeración: ● true ● false
crawler_scanner	Boolean	Si la detección antideslizante está activada Valores de enumeración: ● true ● false
crawler_script	Boolean	Si el antideslizador JavaScript está activado Valores de enumeración: ● true ● false
crawler_other	Boolean	Si está activada la comprobación de otro rastreador Valores de enumeración: ● true ● false
webshell	Boolean	Si la detección de webshell está habilitada Valores de enumeración: ● true ● false
cc	Boolean	Si las reglas de protección contra ataques de CC están habilitadas Valores de enumeración: ● true ● false
custom	Boolean	Si la protección precisa está habilitada Valores de enumeración: ● true ● false
whiteblackip	Boolean	Si la protección de listas negras y blancas está habilitada. Valores de enumeración: ● true ● false

Parámetro	Tipo	Descripción
geoip	Boolean	Si el control de acceso de geolocalización está habilitado Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
ignore	Boolean	Si el enmascaramiento de falsa alarma está habilitado. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
privacy	Boolean	Si el enmascaramiento de datos está habilitado Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
antitamper	Boolean	Si la protección contra manipulaciones web está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
antileakage	Boolean	Si la prevención de fugas de información está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
bot_enable	Boolean	Si la mitigación de bots está habilitada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
modulex_enabled	Boolean	Si la protección contra ataques CC para moduleX está habilitada. Esta función se encuentra en la prueba beta abierta (OBT). Durante la OBT, solo se admite el modo de solo registro. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false

Tabla 4-85 BindHost

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio
waf_type	String	Modo de nombre de dominio: nube (modo nube) / premium (modo dedicado)
mode	String	Este parámetro es requerido solamente por el modo dedicado.

Código de estado: 400

Tabla 4-86 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-87 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 403

Tabla 4-88 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-89 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
POST https://{Endpoint}/v1/{project_id}/waf/policy?enterprise_project_id=0
{
  "name" : "demo"
}
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "precise" : false,
    "whiteblackip" : true,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true,
    "modulex_enabled" : false
  },
  "hosts" : [ ],
  "extend" : { },
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ ]
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
403	La cuota de recursos es insuficiente.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.2.3 Consulta de una política por ID

Función

Consulta de una política por ID

URI

GET /v1/{project_id}/waf/policy/{policy_id}

Tabla 4-90 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-91 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-92 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-93 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de política
name	String	Nombre de la política
action	PolicyAction object	Operación
options	PolicyOption object	Opción
level	Integer	Nivel de protección
full_detection	Boolean	Modo de detección en la regla de protección precisa
bind_host	Array of BindHost objects	Información básica sobre el dominio protegido.
timestamp	Long	Hora en que se crea una política
extend	Map<String,String>	Campo extendido.

Tabla 4-94 PolicyAction

Parámetro	Tipo	Descripción
category	String	Nivel de protección. El valor puede ser log o block . log : WAF solo registra eventos. block : WAF bloquea eventos. Valores de enumeración: <ul style="list-style-type: none"> ● block ● log

Tabla 4-95 PolicyOption

Parámetro	Tipo	Descripción
webattack	Boolean	Si la protección web básica está habilitada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
common	Boolean	Si la comprobación general está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler	Boolean	Si la protección antideslizante está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler_engine	Boolean	Si el motor de búsqueda está habilitado Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler_scanner	Boolean	Si la detección antideslizante está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler_script	Boolean	Si el antideslizador JavaScript está activado Valores de enumeración: <ul style="list-style-type: none"> ● true ● false

Parámetro	Tipo	Descripción
crawler_other	Boolean	Si está activada la comprobación de otro rastreador Valores de enumeración: ● true ● false
webshell	Boolean	Si la detección de webshell está habilitada Valores de enumeración: ● true ● false
cc	Boolean	Si las reglas de protección contra ataques de CC están habilitadas Valores de enumeración: ● true ● false
custom	Boolean	Si la protección precisa está habilitada Valores de enumeración: ● true ● false
whiteblackip	Boolean	Si la protección de listas negras y blancas está habilitada. Valores de enumeración: ● true ● false
geoip	Boolean	Si el control de acceso de geolocalización está habilitado Valores de enumeración: ● true ● false
ignore	Boolean	Si el enmascaramiento de falsa alarma está habilitado. Valores de enumeración: ● true ● false
privacy	Boolean	Si el enmascaramiento de datos está habilitado Valores de enumeración: ● true ● false

Parámetro	Tipo	Descripción
antitamper	Boolean	Si la protección contra manipulaciones web está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
antileakage	Boolean	Si la prevención de fugas de información está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
bot_enable	Boolean	Si la mitigación de bots está habilitada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
modulex_enabled	Boolean	Si la protección contra ataques CC para moduleX está habilitada. Esta función se encuentra en la prueba beta abierta (OBT). Durante la OBT, solo se admite el modo de solo registro. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false

Tabla 4-96 BindHost

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio
waf_type	String	Modo de nombre de dominio: cloud (modo de cloud) / premium (modo dedicado)
mode	String	Este parámetro es requerido solamente por el modo dedicado.

Código de estado: 400

Tabla 4-97 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-98 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-99 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}?  
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{  
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",  
  "name" : "demo",  
  "level" : 2,  
  "action" : {  
    "category" : "log",  
    "modulex_category" : "log"  
  },  
  "options" : {  
    "webattack" : true,  
    "common" : true,  
    "crawler" : true,  
    "crawler_engine" : false,  
    "crawler_scanner" : true,  
    "crawler_script" : false,  
  }  
}
```

```

"crawler_other" : false,
"webshell" : false,
"cc" : true,
"custom" : true,
"precise" : false,
"whiteblackip" : true,
"geoip" : true,
"ignore" : true,
"privacy" : true,
"antitamper" : true,
"anticrawler" : false,
"antileakage" : false,
"followed_action" : false,
"bot_enable" : true,
"modulex_enabled" : false
},
"hosts" : [ ],
"extend" : { },
"timestamp" : 1650529538732,
"full_detection" : false,
"bind_host" : [ ],
"share_info" : {
  "is_receiver" : false,
  "provider_display" : {
    "share_count" : 0,
    "accept_count" : 0,
    "process_status" : 0
  }
}
}

```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.2.4 Actualización de una política de protección aplicada a un nombre de dominio

Función

Esta API se utiliza para actualizar la política de protección aplicada a un nombre de dominio.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}

Tabla 4-100 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-101 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa.
hosts	Sí	String	ID de nombre de dominio. Se puede obtener llamando a la API ListHost .

Parámetros de solicitud

Tabla 4-102 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-103 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de política
name	String	Nombre de la política
action	PolicyAction object	Operación

Parámetro	Tipo	Descripción
options	PolicyOption object	Opción
level	Integer	Nivel de protección
full_detection	Boolean	Modo de detección en la regla de protección precisa
bind_host	Array of BindHost objects	Información básica sobre el dominio protegido.
timestamp	Long	Hora en que se crea una política
extend	Map<String,String>	Campo extendido.

Tabla 4-104 PolicyAction

Parámetro	Tipo	Descripción
category	String	Nivel de protección. El valor puede ser log o block . log : WAF solo registra eventos. block : WAF bloquea eventos. Valores de enumeración: <ul style="list-style-type: none"> ● block ● log

Tabla 4-105 PolicyOption

Parámetro	Tipo	Descripción
webattack	Boolean	Si la protección web básica está habilitada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
common	Boolean	Si la comprobación general está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler	Boolean	Si la protección antideslizante está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false

Parámetro	Tipo	Descripción
crawler_engine	Boolean	Si el motor de búsqueda está habilitado Valores de enumeración: ● true ● false
crawler_scanner	Boolean	Si la detección antideslizante está activada Valores de enumeración: ● true ● false
crawler_script	Boolean	Si el antideslizador JavaScript está activado Valores de enumeración: ● true ● false
crawler_other	Boolean	Si está activada la comprobación de otro rastreador Valores de enumeración: ● true ● false
webshell	Boolean	Si la detección de webshell está habilitada Valores de enumeración: ● true ● false
cc	Boolean	Si las reglas de protección contra ataques de CC están habilitadas Valores de enumeración: ● true ● false
custom	Boolean	Si la protección precisa está habilitada Valores de enumeración: ● true ● false
whiteblackip	Boolean	Si la protección de listas negras y blancas está habilitada. Valores de enumeración: ● true ● false

Parámetro	Tipo	Descripción
geoip	Boolean	Si el control de acceso de geolocalización está habilitado Valores de enumeración: ● true ● false
ignore	Boolean	Si el enmascaramiento de falsa alarma está habilitado. Valores de enumeración: ● true ● false
privacy	Boolean	Si el enmascaramiento de datos está habilitado Valores de enumeración: ● true ● false
antitamper	Boolean	Si la protección contra manipulaciones web está activada Valores de enumeración: ● true ● false
antileakage	Boolean	Si la prevención de fugas de información está activada Valores de enumeración: ● true ● false
bot_enable	Boolean	Si la mitigación de bots está habilitada Valores de enumeración: ● true ● false
modulex_enabled	Boolean	Si la protección contra ataques CC para moduleX está habilitada. Esta función se encuentra en la prueba beta abierta (OBT). Durante la OBT, solo se admite el modo de solo registro. Valores de enumeración: ● true ● false

Tabla 4-106 BindHost

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio
waf_type	String	Modo de nombre de dominio: cloud (modo de cloud) / premium (modo dedicado)
mode	String	Este parámetro es requerido solamente por el modo dedicado.

Código de estado: 400

Tabla 4-107 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-108 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-109 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}?
enterprise_project_id=0&hosts=c0268b883a854adc8a2cd352193b0e13
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log",
    "modulex_category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "precise" : false,
    "whiteblackip" : true,
    "gecip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true,
    "modulex_enabled" : false
  },
  "hosts" : [ "c0268b883a854adc8a2cd352193b0e13" ],
  "extend" : { },
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ {
    "id" : "c0268b883a854adc8a2cd352193b0e13",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud"
  } ],
  "share_info" : {
    "is_receiver" : false,
    "provider_display" : {
      "share_count" : 0,
      "accept_count" : 0,
      "process_status" : 0
    }
  }
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.

Código de estado	Descripción
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.2.5 Actualización de una política de protección

Función

Esta API se utiliza para actualizar una política de protección. El cuerpo de la solicitud sólo puede contener la parte que se va a actualizar.

URI

PATCH /v1/{project_id}/waf/policy/{policy_id}

Tabla 4-110 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-111 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-112 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-113 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
name	No	String	Nombre de la política
action	No	PolicyAction object	Operación
options	No	PolicyOption object	Opción

Tabla 4-114 PolicyAction

Parámetro	Obligatorio	Tipo	Descripción
category	No	String	Nivel de protección. El valor puede ser log o block . log : WAF solo registra eventos. block : WAF bloquea eventos. Valores de enumeración: <ul style="list-style-type: none"> ● block ● log

Tabla 4-115 PolicyOption

Parámetro	Obligatorio	Tipo	Descripción
webattack	No	Boolean	Si la protección web básica está habilitada Valores de enumeración: ● true ● false
common	No	Boolean	Si la comprobación general está activada Valores de enumeración: ● true ● false
crawler	No	Boolean	Si la protección antideslizante está activada Valores de enumeración: ● true ● false
crawler_engine	No	Boolean	Si el motor de búsqueda está habilitado Valores de enumeración: ● true ● false
crawler_scanner	No	Boolean	Si la detección antideslizante está activada Valores de enumeración: ● true ● false
crawler_script	No	Boolean	Si el antideslizador JavaScript está activado Valores de enumeración: ● true ● false
crawler_other	No	Boolean	Si está activada la comprobación de otro rastreador Valores de enumeración: ● true ● false

Parámetro	Obligatorio	Tipo	Descripción
webshell	No	Boolean	Si la detección de webshell está habilitada Valores de enumeración: ● true ● false
cc	No	Boolean	Si las reglas de protección contra ataques de CC están habilitadas Valores de enumeración: ● true ● false
custom	No	Boolean	Si la protección precisa está habilitada Valores de enumeración: ● true ● false
whiteblackip	No	Boolean	Si la protección de listas negras y blancas está habilitada. Valores de enumeración: ● true ● false
geoip	No	Boolean	Si el control de acceso de geolocalización está habilitado Valores de enumeración: ● true ● false
ignore	No	Boolean	Si el enmascaramiento de falsa alarma está habilitado. Valores de enumeración: ● true ● false
privacy	No	Boolean	Si el enmascaramiento de datos está habilitado Valores de enumeración: ● true ● false

Parámetro	Obligatorio	Tipo	Descripción
antitamper	No	Boolean	Si la protección contra manipulaciones web está activada Valores de enumeración: ● true ● false
antileakage	No	Boolean	Si la prevención de fugas de información está activada Valores de enumeración: ● true ● false
bot_enable	No	Boolean	Si la mitigación de bots está habilitada Valores de enumeración: ● true ● false
modulex_enabled	No	Boolean	Si la protección contra ataques CC para moduleX está habilitada. Esta función se encuentra en la prueba beta abierta (OBT). Durante la OBT, solo se admite el modo de solo registro. Valores de enumeración: ● true ● false

Parámetros de respuesta

Código de estado: 200

Tabla 4-116 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de política
name	String	Nombre de la política
level	Integer	Nivel de protección
action	PolicyAction object	Operación
options	PolicyOption object	Opción

Parámetro	Tipo	Descripción
hosts	Array of strings	Información básica sobre el dominio protegido.
extend	Map<String,String>	Campo extendido
timestamp	Long	Hora en que se crea una política
full_detection	Boolean	Modo de detección en la regla de protección precisa
bind_host	Array of BindHost objects	Información básica sobre el dominio protegido.

Tabla 4-117 PolicyAction

Parámetro	Tipo	Descripción
category	String	Nivel de protección. El valor puede ser log o block . log : WAF solo registra eventos. block : WAF bloquea eventos. Valores de enumeración: <ul style="list-style-type: none"> ● block ● log

Tabla 4-118 PolicyOption

Parámetro	Tipo	Descripción
webattack	Boolean	Si la protección web básica está habilitada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
common	Boolean	Si la comprobación general está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler	Boolean	Si la protección antideslizante está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false

Parámetro	Tipo	Descripción
crawler_engine	Boolean	Si el motor de búsqueda está habilitado Valores de enumeración: ● true ● false
crawler_scanner	Boolean	Si la detección antideslizante está activada Valores de enumeración: ● true ● false
crawler_script	Boolean	Si el antideslizador JavaScript está activado Valores de enumeración: ● true ● false
crawler_other	Boolean	Si está activada la comprobación de otro rastreador Valores de enumeración: ● true ● false
webshell	Boolean	Si la detección de webshell está habilitada Valores de enumeración: ● true ● false
cc	Boolean	Si las reglas de protección contra ataques de CC están habilitadas Valores de enumeración: ● true ● false
custom	Boolean	Si la protección precisa está habilitada Valores de enumeración: ● true ● false
whiteblackip	Boolean	Si la protección de listas negras y blancas está habilitada. Valores de enumeración: ● true ● false

Parámetro	Tipo	Descripción
geoip	Boolean	Si el control de acceso de geolocalización está habilitado Valores de enumeración: ● true ● false
ignore	Boolean	Si el enmascaramiento de falsa alarma está habilitado. Valores de enumeración: ● true ● false
privacy	Boolean	Si el enmascaramiento de datos está habilitado Valores de enumeración: ● true ● false
antitamper	Boolean	Si la protección contra manipulaciones web está activada Valores de enumeración: ● true ● false
antileakage	Boolean	Si la prevención de fugas de información está activada Valores de enumeración: ● true ● false
bot_enable	Boolean	Si la mitigación de bots está habilitada Valores de enumeración: ● true ● false
modulex_enabled	Boolean	Si la protección contra ataques CC para moduleX está habilitada. Esta función se encuentra en la prueba beta abierta (OBT). Durante la OBT, solo se admite el modo de solo registro. Valores de enumeración: ● true ● false

Tabla 4-119 BindHost

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio
waf_type	String	Modo de nombre de dominio: cloud (modo de cloud) / premium (modo dedicado)
mode	String	Este parámetro es requerido solamente por el modo dedicado.

Código de estado: 400

Tabla 4-120 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-121 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-122 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
PATCH https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}?
enterprise_project_id=0
```

```
{
  "options" : {
    "whiteblackip" : false
  }
}
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "precise" : false,
    "whiteblackip" : false,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true
  },
  "hosts" : [ "c0268b883a854adc8a2cd352193b0e13" ],
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ {
    "id" : "c0268b883a854adc8a2cd352193b0e13",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud"
  } ],
  "share_info" : {
    "is_receiver" : false,
    "provider_display" : {
      "share_count" : 0,
      "accept_count" : 0,
      "process_status" : 0
    }
  }
}
```

Códigos de estado

Código de estado	Descripción
200	OK

Código de estado	Descripción
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.2.6 Eliminación de una política

Función

Eliminar política

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}

Tabla 4-123 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-124 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-125 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-126 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de política
name	String	Nombre de la política
level	Integer	Nivel de protección
action	PolicyAction object	Operación
options	PolicyOption object	Opción
full_detection	Boolean	Modo de detección en la regla de protección precisa
hosts	Array of strings	ID del sitio web protegido
bind_host	Array of BindHost objects	Información del sitio web protegido
timestamp	Long	Hora en que se crea una política
extend	Object	Campo extendido.

Tabla 4-127 PolicyAction

Parámetro	Tipo	Descripción
category	String	Nivel de protección. El valor puede ser log o block . log : WAF solo registra eventos. block : WAF bloquea eventos. Valores de enumeración: <ul style="list-style-type: none"> ● block ● log

Tabla 4-128 PolicyOption

Parámetro	Tipo	Descripción
webattack	Boolean	Si la protección web básica está habilitada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
common	Boolean	Si la comprobación general está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler	Boolean	Si la protección antideslizante está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler_engine	Boolean	Si el motor de búsqueda está habilitado Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler_scanner	Boolean	Si la detección antideslizante está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
crawler_script	Boolean	Si el antideslizador JavaScript está activado Valores de enumeración: <ul style="list-style-type: none"> ● true ● false

Parámetro	Tipo	Descripción
crawler_other	Boolean	Si está activada la comprobación de otro rastreador Valores de enumeración: ● true ● false
webshell	Boolean	Si la detección de webshell está habilitada Valores de enumeración: ● true ● false
cc	Boolean	Si las reglas de protección contra ataques de CC están habilitadas Valores de enumeración: ● true ● false
custom	Boolean	Si la protección precisa está habilitada Valores de enumeración: ● true ● false
whiteblackip	Boolean	Si la protección de listas negras y blancas está habilitada. Valores de enumeración: ● true ● false
geoip	Boolean	Si el control de acceso de geolocalización está habilitado Valores de enumeración: ● true ● false
ignore	Boolean	Si el enmascaramiento de falsa alarma está habilitado. Valores de enumeración: ● true ● false
privacy	Boolean	Si el enmascaramiento de datos está habilitado Valores de enumeración: ● true ● false

Parámetro	Tipo	Descripción
antitamper	Boolean	Si la protección contra manipulaciones web está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
antileakage	Boolean	Si la prevención de fugas de información está activada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
bot_enable	Boolean	Si la mitigación de bots está habilitada Valores de enumeración: <ul style="list-style-type: none"> ● true ● false
modulex_enabled	Boolean	Si la protección contra ataques CC para moduleX está habilitada. Esta función se encuentra en la prueba beta abierta (OBT). Durante la OBT, solo se admite el modo de solo registro. Valores de enumeración: <ul style="list-style-type: none"> ● true ● false

Tabla 4-129 BindHost

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio
waf_type	String	Modo de nombre de dominio: nube (modo nube) / premium (modo dedicado)
mode	String	Este parámetro es requerido solamente por el modo dedicado.

Código de estado: 400

Tabla 4-130 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-131 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-132 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}?  
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{  
  "id" : "62169e2fc4e64148b775ec01b24a1947",  
  "name" : "demo",  
  "level" : 2,  
  "action" : {  
    "category" : "log",  
    "modulex_category" : "log"  
  },  
  "options" : {  
    "webattack" : true,  
    "common" : true,  
    "crawler" : true,  
    "crawler_engine" : false,  
    "crawler_scanner" : true,  
    "crawler_script" : false,  
  }  
}
```

```

"crawler_other" : false,
"webshell" : false,
"cc" : true,
"custom" : true,
"precise" : false,
"whiteblackip" : true,
"geoip" : true,
"ignore" : true,
"privacy" : true,
"antitamper" : true,
"anticrawler" : false,
"antileakage" : false,
"followed_action" : false,
"bot_enable" : true,
"modulex_enabled" : false
},
"hosts" : [ ],
"extend" : { },
"timestamp" : 1649316510603,
"full_detection" : false,
"bind_host" : [ ]
}

```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error del servidor interno

Códigos de error

Consulte [Códigos de error](#).

4.3 Gestión de reglas

4.3.1 Eliminación de una regla de enmascaramiento de falsa alarma

Función

Esta API se utiliza para eliminar una regla de enmascaramiento de falsa alarma.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}

Tabla 4-133 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .
rule_id	Sí	String	ID de una regla de enmascaramiento de falsa alarma. Puede obtener el ID de regla del campo id en el cuerpo de respuesta de la API ListIgnoreRule que se utiliza para consultar reglas de enmascaramiento de falsas alarmas.

Tabla 4-134 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Puede obtener el ID llamando a la API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-135 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-136 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la regla
policyid	String	ID de política
timestamp	Long	Tiempo de creación de reglas.
description	String	Descripción de la regla
status	Integer	Estado de la regla. El valor puede ser 0 (deshabilitado) o 1 (habilitado).
url	String	La ruta para falsas alarmas de enmascaramiento. Este parámetro sólo está disponible cuando el modo se establece en 0 .
rule	String	ID de la regla integrada que se va a enmascarar. Puede consultar el ID de regla seleccionando Policies > Policy Name > Basic Web Protection > Protection Rules en la consola WAF o en la página de detalles del evento.
mode	Integer	Número de versión. El valor puede ser 0 o 1 . 0 : indica la versión anterior V1. 1 indica la nueva versión V2. Cuando el valor de modo es 0 , el campo conditions no existe, pero existen los campos conditions y conditions . Cuando el valor de modo es 1 , los campos url y url_logic no existen, pero el campo conditions existe.
url_logic	String	Lógica de coincidencia de URL
conditions	Array of Condition objects	Condición
domains	Array of strings	Nombre de dominio o sitio web protegido

Tabla 4-137 Condición

Parámetro	Tipo	Descripción
category	String	Tipo de campo. El valor puede ser ip , url , params , cookie , o header .

Parámetro	Tipo	Descripción
contents	Array of strings	Contenido. La longitud de la matriz está limitada a 1 . El formato de contenido varía según el tipo de campo. Por ejemplo, si el tipo de campo es ip , el valor debe ser una dirección IP o un intervalo de direcciones IP. Si el tipo de campo es url , el valor debe estar en el formato de URL estándar. Si el tipo de campo es params , cookie o header , el formato de contenido no está limitado.
logic_operation	String	La lógica de coincidencia varía dependiendo del tipo de campo. Por ejemplo, si el tipo de campo es ip , la lógica puede ser equal o not_equal . Si el tipo de campo es url , params , cookie , o header , la lógica puede ser equal , not_equal , contain , not_contain , prefix , not_prefix , suffix , not_suffix , regular_match , or regular_not_match .
check_all_indexes_logic	Integer	Si el tipo de campo es url o ip , el campo check_all_indexes_logic no existe. En otros casos, 1 indica que se comprueban todos los subcampos, 2 indica que se comprueba cualquier subcampo, y el null indica que se usan subcampos definidos por el usuario.
index	String	Si el tipo de campo es ip y el subcampo es la dirección IP del cliente, el parámetro index no existe. Si el tipo de subcampo es X-Forwarded-For , el valor es x-forwarded-for . Si el tipo de campo es params , header , or cookie y el subcampo está definido por el usuario, el valor de index es el subcampo definido por el usuario.

Código de estado: 400

Tabla 4-138 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-139 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-140 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}
```

Ejemplo de respuestas

Código de estado: 200

Solicitud realizada

```
{
  "id" : "40484384970948d79fffe4e4ae1fc54d",
  "policyid" : "f385eceedf7c4c34a4d1def19eafbe85",
  "timestamp" : 1650512535222,
  "description" : "demo",
  "status" : 1,
  "rule" : "091004",
  "mode" : 1,
  "conditions" : [ {
    "category" : "ip",
    "contents" : [ "x.x.x.x" ],
    "logic_operation" : "equal"
  } ],
  "domain" : [ "we.test.418lab.cn" ]
}
```

Códigos de estado

Código de estado	Descripción
200	Solicitud realizada
400	Error de solicitud.
401	El token no tiene permisos necesarios.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.3.2 Consulta de la lista de reglas de enmascaramiento de falsa alarma

Función

Esta API se utiliza para consultar la lista de reglas de enmascaramiento de falsas alarmas.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/ignore

Tabla 4-141 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-142 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.
page	No	Integer	Número de página de los datos a devolver durante la consulta de paginación. El valor varía de 0 a 100000 . El valor predeterminado es 1 , que indica que se devuelven los datos de la primera página. Predeterminado: 1
pagesize	No	Integer	Número de resultados en cada página durante la consulta de paginación. El valor varía de 1 a 100 . El valor predeterminado es 10 , lo que indica que cada página contiene 10 resultados. Predeterminado: 10

Parámetros de solicitud

Tabla 4-143 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-144 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Número de reglas de enmascaramiento de falsas alarmas en la política
items	Array of IgnoreRuleBody objects	Objetos de regla de enmascaramiento de falsa alarma

Tabla 4-145 IgnoreRuleBody

Parámetro	Tipo	Descripción
id	String	ID de la regla
policyid	String	ID de política
timestamp	Long	Tiempo de creación de reglas.
description	String	Descripción de la regla
status	Integer	Estado de la regla. El valor puede ser 0 (deshabilitado) o 1 (habilitado).
url	String	La ruta para falsas alarmas de enmascaramiento. Este parámetro sólo está disponible cuando el modo se establece en 0 .

Parámetro	Tipo	Descripción
rule	String	ID de la regla integrada que se va a enmascarar. Puede consultar el ID de regla seleccionando Policies > Policy Name > Basic Web Protection > Protection Rules en la consola WAF o en la página de detalles del evento.
mode	Integer	Número de versión. El valor puede ser 0 o 1 . 0 : indica la versión anterior V1. 1 indica la nueva versión V2. Cuando el valor de modo es 0 , el campo conditions no existe, pero existen los campos conditions y conditions . Cuando el valor de modo es 1 , los campos url y url_logic no existen, pero el campo conditions existe.
url_logic	String	Lógica de coincidencia. El valor puede ser equal , not_equal , contain , not_contain , prefix , not_prefix , suffix , not_suffix , regular_match , o regular_not_match .
conditions	Array of Condition objects	Lista de condiciones
domains	Array of strings	Nombre de dominio o sitio web protegido

Tabla 4-146 Condición

Parámetro	Tipo	Descripción
category	String	Tipo de campo. El valor puede ser ip , url , params , cookie , o header .
contents	Array of strings	Contenido. La longitud de la matriz está limitada a 1 . El formato de contenido varía según el tipo de campo. Por ejemplo, si el tipo de campo es ip , el valor debe ser una dirección IP o un intervalo de direcciones IP. Si el tipo de campo es url , el valor debe estar en el formato de URL estándar. Si el tipo de campo es params , cookie o header , el formato de contenido no está limitado.
logic_operation	String	La lógica de coincidencia varía dependiendo del tipo de campo. Por ejemplo, si el tipo de campo es ip , la lógica puede ser equal o not_equal . Si el tipo de campo es url , params , cookie , o header , la lógica puede ser equal , not_equal , contain , not_contain , prefix , not_prefix , suffix , not_suffix , regular_match , or regular_not_match .

Parámetro	Tipo	Descripción
check_all_indexes_logic	Integer	Si el tipo de campo es url o ip , el campo check_all_indexes_logic no existe. En otros casos, 1 indica que se comprueban todos los subcampos, 2 indica que se comprueba cualquier subcampo, y el null indica que se usan subcampos definidos por el usuario.
index	String	Si el tipo de campo es ip y el subcampo es la dirección IP del cliente, el parámetro index no existe. Si el tipo de subcampo es X-Forwarded-For , el valor es x-forwarded-for . Si el tipo de campo es params , header , or cookie y el subcampo está definido por el usuario, el valor de index es el subcampo definido por el usuario.

Código de estado: 400

Tabla 4-147 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 403

Tabla 4-148 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-149 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-150 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/ignore?
enterprise_project_id=0&page=1&pagesize=10
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "40484384970948d79fffe4e4ae1fc54d",
    "policyid" : "f385eceedf7c4c34a4d1def19eafbe85",
    "timestamp" : 1650512535222,
    "description" : "demo",
    "status" : 1,
    "rule" : "091004",
    "mode" : 1,
    "conditions" : [ {
      "category" : "ip",
      "contents" : [ "x.x.x.x" ],
      "logic_operation" : "equal"
    } ],
    "domain" : [ "we.test.418lab.cn" ]
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
403	La cuota de recursos es insuficiente.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.3.3 Adición de una regla de enmascaramiento de falsa alarma

Función

Esta API se utiliza para agregar una regla de enmascaramiento de falsa alarma.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/ignore

Tabla 4-151 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-152 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Puede obtener el ID llamando a la API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-153 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-154 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
domain	Sí	Array of strings	Nombre de dominio o sitio web a proteger. Si la longitud del array es 0 , la regla entra en vigor para todos los nombres de dominio o sitios web.
conditions	Sí	Array of CreateCondition objects	Lista de condiciones
mode	Sí	Integer	El valor se fija en 1 , indicando v2 reglas de enmascaramiento de falsa alarma. v1 se utiliza solo para la compatibilidad con versiones anteriores, y las reglas de falsa alarma no se pueden crear en v1.
rule	Sí	String	ID de las reglas de enmascaramiento de falsas alarmas incorporadas. Puede consultar el ID de regla seleccionando Policies > Policy Name > Basic Web Protection > Protection Rules en la consola WAF o en la página de detalles del evento.
description	No	String	Descripción de la regla de filtrado

Tabla 4-155 CreateCondition

Parámetro	Obligatorio	Tipo	Descripción
category	Sí	String	Tipo de campo. El valor puede ser ip, url, params, cookie, o header .
contents	Sí	Array of strings	Contenido. La longitud de la matriz está limitada a 1 . El formato de contenido varía según el tipo de campo. Por ejemplo, si el tipo de campo es ip , el valor debe ser una dirección IP o un intervalo de direcciones IP. Si el tipo de campo es url , el valor debe estar en el formato de URL estándar. Si el tipo de campo es params, cookie o header , el formato de contenido no está limitado.

Parámetro	Obligatorio	Tipo	Descripción
logic_operation	Sí	String	La lógica de coincidencia varía dependiendo del tipo de campo. Por ejemplo, si el tipo de campo es ip , la lógica puede ser equal o not_equal . Si el tipo de campo es url , params , cookie , o header , la lógica puede ser equal , not_equal , contain , not_contain , prefix , not_prefix , suffix , not_suffix , regular_match , or regular_not_match .
check_all_indexes_logic	No	Integer	Solo cuando se utiliza un subcampo definido por el usuario y el tipo de campo es url o ip , el parámetro check_all_indexes_logic no es necesario. En otros casos, su valor puede ser 1 o 2 , 1 : indica que todos los subcampos están marcados. 2 indica que se comprueba cualquiera de los subcampos.
index	No	String	Si el tipo de campo es ip y el subcampo es la dirección IP del cliente, el parámetro index no es necesario. Si el tipo de subcampo es X-Forwarded-For , el valor es x-forwarded-for . Si el tipo de campo es params , header , or cookie y el subcampo está definido por el usuario, el valor de index es el subcampo definido por el usuario.

Parámetros de respuesta

Código de estado: 200

Tabla 4-156 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la regla
policyid	String	ID de política
timestamp	Long	Tiempo de creación de reglas.

Parámetro	Tipo	Descripción
description	String	Descripción de la regla
status	Integer	Estado de la regla. El valor puede ser 0 (deshabilitado) o 1 (habilitado).
rule	String	ID de la regla integrada que se va a enmascarar. Puede consultar el ID de regla seleccionando Policies > Policy Name > Basic Web Protection > Protection Rules en la consola WAF o en la página de detalles del evento.
mode	Integer	El valor se fija en 1 , lo que indica que se usan las reglas de enmascaramiento de falsas alarmas v2. v1 se utiliza solo para la compatibilidad con versiones anteriores, y las reglas de falsa alarma no se pueden crear en v1.
conditions	Array of Condition objects	Lista de condiciones
domain	Array of strings	Nombre de dominio o sitio web protegido

Tabla 4-157 Condición

Parámetro	Tipo	Descripción
category	String	Tipo de campo. El valor puede ser ip , url , params , cookie , o header .
contents	Array of strings	Contenido. La longitud de la matriz está limitada a 1 . El formato de contenido varía según el tipo de campo. Por ejemplo, si el tipo de campo es ip , el valor debe ser una dirección IP o un intervalo de direcciones IP. Si el tipo de campo es url , el valor debe estar en el formato de URL estándar. Si el tipo de campo es params , cookie o header , el formato de contenido no está limitado.
logic_operation	String	La lógica de coincidencia varía dependiendo del tipo de campo. Por ejemplo, si el tipo de campo es ip , la lógica puede ser equal o not_equal . Si el tipo de campo es url , params , cookie , o header , la lógica puede ser equal , not_equal , contain , not_contain , prefix , not_prefix , suffix , not_suffix , regular_match , or regular_not_match .

Parámetro	Tipo	Descripción
check_all_indexes_logic	Integer	Si el tipo de campo es url o ip , el campo check_all_indexes_logic no existe. En otros casos, 1 indica que se comprueban todos los subcampos, 2 indica que se comprueba cualquier subcampo, y el null indica que se usan subcampos definidos por el usuario.
index	String	Si el tipo de campo es ip y el subcampo es la dirección IP del cliente, el parámetro index no existe. Si el tipo de subcampo es X-Forwarded-For , el valor es x-forwarded-for . Si el tipo de campo es params , header , or cookie y el subcampo está definido por el usuario, el valor de index es el subcampo definido por el usuario.

Código de estado: 400

Tabla 4-158 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-159 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-160 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/ignore?
enterprise_project_id=0

{
  "domain" : [ "we.test.418lab.cn" ],
  "conditions" : [ {
    "category" : "url",
    "logic_operation" : "contain",
    "contents" : [ "x.x.x.x" ],
    "index" : null
  } ],
  "mode" : 1,
  "description" : "demo",
  "rule" : "091004"
}
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "a57f20ced01e4e0d8bea8e7c49eea254",
  "policyid" : "f385eceedf7c4c34a4d1def19eafbe85",
  "timestamp" : 1650522310447,
  "description" : "demo",
  "status" : 1,
  "rule" : "091004",
  "mode" : 1,
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "x.x.x.x" ],
    "logic_operation" : "contain"
  } ],
  "domain" : [ "we.test.418lab.cn" ]
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	El token no tiene permisos necesarios.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.3.4 Consulta de la lista de tablas de referencia

Función

Esta API se utiliza para consultar la lista de tablas de referencia.

URI

GET /v1/{project_id}/waf/valuelist

Tabla 4-161 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-162 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
page	No	Integer	Número de página de los datos a devolver durante la consulta de paginación. El valor varía de 0 a 100000 . El valor predeterminado es 1 , que indica que se devuelven los datos de la primera página.
pagesize	No	Integer	Número de resultados en cada página durante la consulta de paginación. El valor varía de 1 a 100 . El valor predeterminado es 10 , lo que indica que cada página contiene 10 resultados.
name	No	String	Nombre de tabla de referencia

Parámetros de solicitud

Tabla 4-163 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).

Parámetro	Obligatorio	Tipo	Descripción
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-164 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Número de tablas de referencia Mínimo: 0 Máximo: 500
items	Array of ValueListResponseBody objects	Lista de tablas de referencia

Tabla 4-165 ValueListResponseBody

Parámetro	Tipo	Descripción
id	String	ID de la tabla de referencia
name	String	Nombre de tabla de referencia.
type	String	Tipo de tabla de referencia
timestamp	Long	Marca de tiempo de la tabla de referencia
values	Array of strings	Valor de la tabla de referencia
producer	Integer	Fuente de la tabla de referencia. El valor puede ser 1 u otros. 1 : La tabla es creada por los usuarios. Otros valores indican que la tabla es generada automáticamente por modulleX.
description	String	Descripción de la tabla de referencia

Código de estado: 400

Tabla 4-166 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-167 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-168 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/valuelist?enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "total" : 1,
  "items" : [ {
    "id" : "3b03be27a40b45d3b21fe28a351e2021",
    "name" : "ip_list848",
    "type" : "ip",
    "values" : [ "100.100.100.125" ],
    "timestamp" : 1650421866870,
    "producer" : 1,
    "description" : "demo"
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error del servidor interno

Códigos de error

Consulte [Códigos de error](#).

4.3.5 Creación de una tabla de referencia

Función

Esta API se utiliza para crear una tabla de referencia.

URI

POST /v1/{project_id}/waf/valuelist

Tabla 4-169 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-170 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-171 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-172 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
name	Sí	String	Nombre de tabla de referencia. El valor puede contener un máximo de 64 caracteres. Solo se permiten dígitos, letras, guiones (-) guiones bajos y puntos (.). Mínimo: 2 Máximo: 64
type	Sí	String	Tipo de tabla de referencia. Para obtener más información, consulte la lista de enumeración. Mínimo: 2 Máximo: 32 Valores de enumeración: <ul style="list-style-type: none"> ● url ● params ● ip ● cookie ● referer ● user-agent ● header ● response_code ● response_header ● response_body
values	Sí	Array of strings	Valor de la tabla de referencia

Parámetro	Obligatorio	Tipo	Descripción
description	No	String	Descripción de la tabla de referencia. El valor contiene un máximo de 128 caracteres. Mínimo: 0 Máximo: 128

Parámetros de respuesta

Código de estado: 200

Tabla 4-173 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la tabla de referencia
name	String	Nombre de tabla de referencia
type	String	Tipo de tabla de referencia
description	String	Descripción de la tabla de referencia
timestamp	Long	Marca de tiempo de la tabla de referencia
values	Array of strings	Valor de la tabla de referencia

Código de estado: 400

Tabla 4-174 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-175 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-176 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
POST https://{Endpoint}/v1/{project_id}/waf/valueList?enterprise_project_id=0
{
  "name" : "demo",
  "type" : "url",
  "values" : [ "/124" ],
  "description" : "demo"
}
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "id" : "e5d9032d8da64d169269175c3e4c2849",
  "name" : "demo",
  "type" : "url",
  "values" : [ "/124" ],
  "timestamp" : 1650524684892,
  "description" : "demo",
  "producer" : 1
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error del servidor interno

Códigos de error

Consulte [Códigos de error](#).

4.3.6 Modificación de una tabla de referencia

Función

Esta API se utiliza para modificar una tabla de referencia.

URI

PUT /v1/{project_id}/waf/valuelist/{valuelistid}

Tabla 4-177 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
valuelistid	Sí	String	ID. de la tabla de referencia. Se puede obtener llamando a la API ListValueList .

Tabla 4-178 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-179 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-180 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
name	Sí	String	Nombre de la tabla de referencia, que es una cadena de 2 a 32 caracteres. Mínimo: 2 Máximo: 32
type	Sí	String	Tipo de tabla de referencia. Para obtener más información, consulte la lista de enumeración. Mínimo: 2 Máximo: 32 Valores de enumeración: <ul style="list-style-type: none"> ● url ● params ● ip ● cookie ● referer ● user-agent ● header ● response_code ● response_header ● resopnse_body
values	No	Array of strings	Valor de la tabla de referencia
description	No	String	Descripción de la tabla de referencia. El valor contiene un máximo de 128 caracteres. Mínimo: 0 Máximo: 128

Parámetros de respuesta

Código de estado: 200

Tabla 4-181 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la tabla de referencia
name	String	Nombre de tabla de referencia.

Parámetro	Tipo	Descripción
type	String	Tipo de tabla de referencia
description	String	Descripción de la tabla de referencia
timestamp	Long	Marca de tiempo de la tabla de referencia
values	Array of strings	Valor de la tabla de referencia
producer	Integer	Fuente de la tabla de referencia. \n - 1 : La tabla se crea manualmente.\n - 2 La tabla se crea automáticamente por moduleX.

Código de estado: 400

Tabla 4-182 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-183 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-184 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
PUT https://{Endpoint}/v1/{project_id}/waf/valuelist/{valuelistid}?
enterprise_project_id=0
```

```
{
  "name" : "RPmvp0m4",
  "type" : "response_code",
  "values" : [ "500" ],
  "description" : "demo"
}
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "id" : "63b1d9edf2594743bc7c6ee98527306c",
  "name" : "RPmvp0m4",
  "type" : "response_code",
  "values" : [ "500" ],
  "description" : "demo",
  "producer" : 1
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.3.7 Eliminación de una tabla de referencia

Función

Esta API se utiliza para eliminar una tabla de referencia.

URI

DELETE /v1/{project_id}/waf/valuelist/{valuelistid}

Tabla 4-185 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Parámetro	Obligatorio	Tipo	Descripción
valuelistid	Sí	String	ID de la tabla de referencia. Se puede obtener llamando a la API ListValueList .

Tabla 4-186 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-187 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-188 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la tabla de referencia
name	String	Nombre de tabla de referencia.
type	String	Tipo de tabla de referencia
timestamp	Long	Hora en que se suprime la tabla de referencia. El valor es una marca de tiempo de 13 dígitos en milisegundos.

Código de estado: 400

Tabla 4-189 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-190 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-191 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
DELETE https://{Endpoint}/v1/{project_id}/waf/valuelist/{valuelistid}?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "id" : "63b1d9edf2594743bc7c6ee98527306c",
  "name" : "Rpmvp0m4",
  "type" : "response_code",
  "timestamp" : 1640938602391
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.3.8 Cambio del estado de una regla

Función

Esta API se utiliza para cambiar el estado de una regla.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/{ruletype}/{rule_id}/status

Tabla 4-192 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API para consultar la lista de políticas.
ruletype	Sí	String	Tipo Valores de enumeración: <ul style="list-style-type: none"> ● whiteblackip ● geoip ● privacy ● antitamper

Parámetro	Obligatorio	Tipo	Descripción
rule_id	Yes	String	ID de la regla. Se puede obtener llamando a la API específica que se utiliza para obtener la lista de reglas de un tipo de protección determinado. Por ejemplo, puedes llamar a la API ListWhiteblackipRule para obtener el ID de una regla de lista negra o lista blanca.

Tabla 4-193 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa.

Parámetros de solicitud

Tabla 4-194 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-195 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
status	No	Integer	Estado. Las opciones son 0 y 1 . 0 : Desactivado. 1 : Habilitado.

Parámetros de respuesta

Código de estado: 200

Tabla 4-196 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la regla
policyid	String	ID de política
timestamp	Long	Hora en que se creó la regla.
description	String	Descripción de la regla
status	Integer	Estado. Las opciones son 0 y 1. 0: Desactivado. 1: Habilitado.

Código de estado: 400

Tabla 4-197 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-198 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-199 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/{ruletype}/
{rule_id}/status?enterprise_project_id=0
```

```
{
  "status" : 0
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "709bfd0d62a9410394ffa9e25eb82c36",
  "policyid" : "62fd7f8c36234a4ebedabc2ce451ed45",
  "timestamp" : 1650362797070,
  "description" : "demo",
  "status" : 0
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.3.9 Consulta de la lista de reglas de la lista negra y la lista blanca

Función

Esta API se utiliza para consultar la lista de reglas de listas negras y listas blancas.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip

Tabla 4-200 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-201 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.
page	No	Integer	Número de página de los datos a devolver durante la consulta de paginación. El valor varía de 0 a 100000 . El valor predeterminado es 1 , que indica que se devuelven los datos de la primera página. Predeterminado: 1
pagesize	No	Integer	Número de resultados en cada página durante la consulta de paginación. El valor varía de 1 a 100 . El valor predeterminado es 10 , lo que indica que cada página contiene 10 resultados. Predeterminado: 10
name	No	String	ID de la regla de lista negra o lista blanca

Parámetros de solicitud

Tabla 4-202 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-203 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Cantidad de reglas
items	Array of WhiteBlackIpResponseBody objects	Reglas

Tabla 4-204 WhiteBlackIpResponseBody

Parámetro	Tipo	Descripción
id	String	ID de la regla.
policyid	String	ID de política
timestamp	Long	Tiempo de creación de reglas.
description	String	Descripción de la regla
status	Integer	Estado de la regla. El valor puede ser 0 (deshabilitado) o 1 (habilitado).
addr	String	Listas negras y blancas
white	Integer	Acción protectora: \n - 0 : Block \n - 1 : Allow \n - 2 : Log only

Código de estado: 400

Tabla 4-205 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-206 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-207 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "3c96caf769ca4f57814fcf4259ea89a1",
    "policyid" : "4dddfd44fc89453e9fd9cd6bfdc39db2",
    "policyname" : "hkhtest",
    "timestamp" : 1650362891844,
    "description" : "demo",
    "status" : 1,
    "addr" : "x.x.x.x",
    "white" : 0
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error del servidor interno

Códigos de error

Consulte [Códigos de error](#).

4.3.10 Creación de una regla de lista negra/lista blanca

Función

Esta API se utiliza para crear una regla de lista negra o lista blanca.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/whiteblackip

Tabla 4-208 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-209 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-210 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-211 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
name	Sí	String	El nombre de la regla contiene un máximo de 64 caracteres. Solo se permiten letras, dígitos, guiones bajos (_) y puntos (.).
addr	Sí	String	Direcciones IP o intervalos de direcciones IP en la regla de lista negra o lista blanca, por ejemplo, 42.123.120.66 o 42.123.120.0/16.
description	No	String	Descripción de la regla
white	Sí	Integer	Acción protectora: \n - 0 : Block \n - 1 : Allow \n - 2 : Log only

Parámetros de respuesta

Código de estado: 200

Tabla 4-212 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la regla.
policyid	String	ID de política
addr	String	Direcciones IP o intervalos de direcciones IP en la regla de lista negra o lista blanca, por ejemplo, 42.123.120.66 o 42.123.120.0/16.
white	Integer	Acción protectora: \n - 0 : Block \n - 1 : Allow \n - 2 : Log only
timestamp	Long	Hora en que se crea una regla. El valor es una marca de tiempo de 13 dígitos en milisegundos.

Código de estado: 400

Tabla 4-213 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-214 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-215 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip?
enterprise_project_id=0

{
  "name" : "demo",
  "white" : 0,
  "description" : "demo",
  "addr" : "x.x.x.x"
}
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "5d43af25404341058d5ab17b7ba78b56",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650531872900,
  "description" : "demo",
  "status" : 1,
  "addr" : "x.x.x.x",
  "white" : 0,
  "size" : 1
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error del servidor interno

Códigos de error

Consulte [Códigos de error](#).

4.3.11 Actualización de una regla de protección de listas negras o blancas

Función

Esta API se utiliza para actualizar una regla de lista negra o lista blanca.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}

Tabla 4-216 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .
rule_id	Sí	String	ID de la regla de lista negra o lista blanca. Se puede obtener llamando a la API ListWhiteblackipRule .

Tabla 4-217 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-218 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-219 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
name	Sí	String	Nombre de la regla
addr	Sí	String	Direcciones IP o intervalos de direcciones IP en la regla de lista negra o lista blanca, por ejemplo, 42.123.120.66 o 42.123.120.0/16.
description	No	String	Descripción de la regla de la lista negra o de la lista blanca
white	Yes	Integer	Acción protectora: \n - 0 : Block \n - 1 : Allow \n - 2 : Log only

Parámetros de respuesta

Código de estado: 200

Tabla 4-220 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la regla.
policyid	String	ID de política
addr	String	Direcciones IP en la regla de la lista negra o de la lista blanca
description	String	Descripción de la regla de la lista negra o la lista blanca

Parámetro	Tipo	Descripción
Blanco	entera	Acción protectora: \n - 0: Block \n - 1: Allow \n - 2: Log only

Código de estado: 400

Tabla 4-221 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-222 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-223 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip?
enterprise_project_id=0

{
  "name" : "demo",
  "white" : 0,
  "description" : "demo",
  "addr" : "1.1.1.2"
}
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "5d43af25404341058d5ab17b7ba78b56",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650531872900,
  "description" : "demo",
  "status" : 1,
  "addr" : "1.1.1.2",
  "white" : 0
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error del servidor interno

Códigos de error

Consulte [Códigos de error](#).

4.3.12 Eliminación de una regla de lista negra o de lista blanca

Función

Esta API se utiliza para eliminar una regla de lista negra o lista blanca.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}

Tabla 4-224 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Parámetro	Obligatorio	Tipo	Descripción
rule_id	Sí	String	ID de la regla de lista negra o lista blanca. Se puede obtener llamando a la API ListWhiteblackipRule .

Tabla 4-225 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-226 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-227 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de regla de lista negra o blanca
policyid	String	ID de política
name	String	Nombre de la regla
timestamp	Long	Hora en que se elimina una regla. El valor debe ser una marca de tiempo de 13 dígitos en milisegundos.
description	String	Descripción.

Parámetro	Tipo	Descripción
status	Integer	Estado de la regla. El valor puede ser 0 (deshabilitado) o 1 (habilitado).
addr	String	Direcciones IP o intervalos de direcciones IP en la regla de lista negra o lista blanca, por ejemplo, 42.123.120.66 o 42.123.120.0/16.
white	Integer	Acción protectora: \n - 0 : Block \n - 1 : Allow \n - 2 : Log only

Código de estado: 400

Tabla 4-228 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-229 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-230 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip?enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "id" : "5d43af25404341058d5ab17b7ba78b56",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650531872900,
  "description" : "demo",
  "status" : 1,
  "addr" : "1.1.1.2",
  "white" : 0
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error del servidor interno

Códigos de error

Consulte [Códigos de error](#).

4.3.13 Creación de una regla de enmascaramiento de datos

Función

Esta API se utiliza para crear una regla de enmascaramiento de datos.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/privacy

Tabla 4-231 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-232 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-233 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-234 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
url	Sí	String	URL protegida por la regla de enmascaramiento de datos. El valor debe estar en el formato de URL estándar, por ejemplo, /admin/xxx o /admin/. El asterisco () indica el prefijo de ruta.
category	Sí	String	Campo enmascarado Valores de enumeración: <ul style="list-style-type: none"> ● params ● cookie ● header ● form
index	Sí	String	Nombre del campo enmascarado
description	No	String	Descripción de la regla

Parámetros de respuesta

Código de estado: 200

Tabla 4-235 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la regla.
policyid	String	ID de política
url	String	URL protegida por la regla de enmascaramiento de datos. El valor debe estar en el formato de URL estándar, por ejemplo, /admin/xxx o /admin/. El asterisco (*) indica el prefijo de ruta.
category	String	Campo enmascarado Valores de enumeración: <ul style="list-style-type: none"> ● params ● cookie ● header ● form
index	String	Nombre del campo enmascarado

Código de estado: 400

Tabla 4-236 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-237 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-238 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy?
enterprise_project_id=0

{
  "url" : "/demo",
  "category" : "cookie",
  "index" : "demo",
  "description" : "demo"
}
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "id" : "97e4d35f375f4736a21cccfad77613eb",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "timestamp" : 1650533191385,
  "description" : "demo",
  "status" : 1,
  "url" : "/demo",
  "category" : "cookie",
  "index" : "demo"
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error del servidor interno

Códigos de error

Consulte [Códigos de error](#).

4.3.14 Consulta de una regla de enmascaramiento de datos

Función

Esta API se utiliza para consultar una regla de enmascaramiento de datos.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/privacy

Tabla 4-239 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-240 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.
page	No	Integer	Número de página de los datos a devolver durante la consulta de paginación. El valor varía de 0 a 100000 . El valor predeterminado es 1 , que indica que se devuelven los datos de la primera página.
pagesize	No	Integer	Número de resultados en cada página durante la consulta de paginación. El valor varía de 1 a 100 . El valor predeterminado es 10 , lo que indica que cada página contiene 10 resultados.

Parámetros de solicitud

Tabla 4-241 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-242 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Cantidad de reglas
items	Array of PrivacyResponseBody objects	Reglas

Tabla 4-243 PrivacyResponseBody

Parámetro	Tipo	Descripción
id	String	ID de la regla.
policyid	String	ID de política
timestamp	Long	Hora en que se crea una regla. El valor es una marca de tiempo de 13 dígitos en milisegundos.
status	Integer	Estado de la regla. El valor puede ser 0 (deshabilitado) o 1 (habilitado).
url	String	URL protegida por la regla de enmascaramiento de datos

Parámetro	Tipo	Descripción
category	String	Campo enmascarado Valores de enumeración: <ul style="list-style-type: none"> ● params ● cookie ● header ● form
index	String	Nombre del campo enmascarado

Código de estado: 400

Tabla 4-244 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-245 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-246 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "total" : 1,
  "items" : [ {
    "id" : "97e4d35f375f4736a21cccfad77613eb",
    "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
    "policyname" : "demo",
    "timestamp" : 1650533191385,
    "description" : "demo",
    "status" : 1,
    "url" : "/demo",
    "category" : "cookie",
    "index" : "demo"
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.3.15 Actualización de una regla de enmascaramiento de datos

Función

Esta API se utiliza para actualizar una regla de enmascaramiento de datos.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}

Tabla 4-247 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Parámetro	Obligatorio	Tipo	Descripción
rule_id	Sí	String	privacyRuleId

Tabla 4-248 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-249 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-250 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
url	Sí	String	URL protegida por la regla de enmascaramiento de datos. El valor debe estar en el formato de URL estándar, por ejemplo, /admin/xxx o /admin/. El asterisco () indica el prefijo de ruta.
category	Sí	String	Campo enmascarado Valores de enumeración: <ul style="list-style-type: none"> ● params ● cookie ● header ● form

Parámetro	Obligatorio	Tipo	Descripción
index	Sí	String	Nombre del campo enmascarado
description	No	String	Descripción de la regla

Parámetros de respuesta

Código de estado: 200

Tabla 4-251 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la regla.
policyid	String	ID de política
url	String	URL protegida por la regla de enmascaramiento de datos
category	String	Campo enmascarado Valores de enumeración: <ul style="list-style-type: none"> ● params ● cookie ● header ● form
index	String	Nombre del campo enmascarado

Código de estado: 400

Tabla 4-252 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-253 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error

Parámetro	Tipo	Descripción
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-254 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}?
enterprise_project_id=0

{
  "url" : "/demo",
  "category" : "cookie",
  "index" : "demo1",
  "description" : "demo"
}
```

Ejemplo de respuestas

Código de estado: 200

Solicitado.

```
{
  "id" : "97e4d35f375f4736a21cccfad77613eb",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "description" : "demo",
  "url" : "/demo",
  "category" : "cookie",
  "index" : "demo1"
}
```

Códigos de estado

Código de estado	Descripción
200	Solicitado.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error del servidor interno

Códigos de error

Consulte [Códigos de error](#).

4.3.16 Eliminación de una regla de enmascaramiento de datos

Función

Esta API se utiliza para eliminar una regla de enmascaramiento de datos.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}

Tabla 4-255 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .
rule_id	Sí	String	ID de la regla de enmascaramiento de datos. Se puede obtener llamando a la API ListPrivacyRule .

Tabla 4-256 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-257 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).

Parámetro	Obligatorio	Tipo	Descripción
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-258 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la regla
policyid	String	ID de política
timestamp	Long	Hora en que se crea la regla.
description	String	Descripción de la regla
status	Integer	Estado de la regla. El valor puede ser 0 o 1 . 0 : Desactivado. 1 : Habilitado.
url	String	Ruta
category	String	Campo enmascarado
index	String	Nombre del campo enmascarado

Código de estado: 400

Tabla 4-259 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-260 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error

Parámetro	Tipo	Descripción
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-261 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}?enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "id" : "97e4d35f375f4736a21cccfad77613eb",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "timestamp" : 1650533191385,
  "description" : "demo",
  "status" : 1,
  "url" : "/demo",
  "category" : "cookie",
  "index" : "demo1"
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error del servidor interno

Códigos de error

Consulte [Códigos de error](#).

4.3.17 Consulta de la lista de reglas de control de acceso de geolocalización

Función

Esta API se utiliza para consultar la lista de reglas de control de acceso de geolocalización.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/geoup

Tabla 4-262 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-263 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.
page	No	Integer	Número de página de los datos a devolver durante la consulta de paginación. El valor varía de 0 a 100000 . El valor predeterminado es 1 , que indica que se devuelven los datos de la primera página. Predeterminado: 1
pagesize	No	Integer	Número de resultados en cada página durante la consulta de paginación. El valor varía de 1 a 100 . El valor predeterminado es 10 , lo que indica que cada página contiene 10 resultados. Predeterminado: 10

Parámetros de solicitud

Tabla 4-264 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-265 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Número de ubicaciones geográficas bloqueadas en la política.
items	Array of GeOIpItem objects	Lista de las ubicaciones bloqueadas en las reglas de control de acceso de geolocalización

Tabla 4-266 GeOIpItem

Parámetro	Tipo	Descripción
id	String	ID de la regla.

Parámetro	Tipo	Descripción
geoip	String	Códigos para regiones que se pueden utilizar en una regla de control de acceso de geolocalización. \n CN : China, AB2 : Fuera de China continental, AB : Fuera de China continental, Hong Kong, Macao y Taiwán, CA : Canadá, US : Los Estados Unidos, AU : Australia, IN : India, JP : Japón, UK : Reino Unido, FR : Francia, DE : Alemania, BR : Brasil, Ukraine : Ucrania, North Korea : Corea del Norte, The Republic of Korea : La República de Corea, Iran : Irán, Cuba : Cuba, Sultan : Sudán, Syria : Siria, Pakistan : Pakistán, Palestine Palestina, Israel Israel, Iraq : Iraq, Afghanistan : Afganistán, Libya : Libia, Turkey : Turquía, Thailand : Tailandia, Singapore : Singapur, South Africa : Sudáfrica, Mexico : México, Peru : Perú, Indonesia : Indonesia, GD Guangdong, FJ : Fujian, JL : Jilin, LN : Liaoning, TW : Taiwan (China), GZ : Guizhou, AH : Anhui, HL : Heilongjiang, HA : Henan, SC : Sichuan, HE : Hebei, YN : Yunnan, HB : Hubei, HI : Hainan, QH : Qinghai, HN : Hunan, JX : Jiangxi, SX : Shanxi, SN : Shaanxi, ZJ : Zhejiang, GS : Gansu, JS : Jiangsu, SD : Shandong, BJ : Beijing, SH : Shanghai, TJ : Tianjin, CQ : Chongqing, MO : Macao (China), HK : Hong Kong (China), NX : Ningxia, GX : Guangxi, XJ : Xinjiang, XZ : Tibet, NM : Mongolia interior
white	Integer	Acción protectora: \n - 0 : Block \n - 1 : Allow \n - 2 : Log only
timestamp	Long	Marca de tiempo de creación de reglas

Código de estado: 400

Tabla 4-267 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-268 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error

Parámetro	Tipo	Descripción
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-269 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/geoip?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "06f07f6c229141b9a4a78614751bb687",
    "policyid" : "2abeecefb9840e6bf05efbd80d0fcd7",
    "policyname" : "policy_LOow3V51",
    "timestamp" : 1636340038062,
    "status" : 1,
    "geoip" : "GD",
    "white" : 1,
    "geoTagList" : [ "GD" ]
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.3.18 Creación de una regla de control de acceso de geolocalización

Función

Esta API se utiliza para crear una regla de control de acceso de geolocalización.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/geoip

Tabla 4-270 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-271 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-272 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-273 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
geoip	Sí	String	Ubicaciones geográficas que se pueden utilizar para el control de acceso. Códigos de ubicación: \n (CN: China, AB2 : Fuera de China, AB : Fuera de China continental, CA : Canadá, US : Estados Unidos, AU : Australia, IN : India, JP : Japón, UK : Reino Unido, FR : Francia, DE : Alemania, BR : Brasil, Ukraine : Ucrania, North Korea : Corea del Norte, The Republic of Korea : Corea del Sur, Iran : Irán, Cuba : Cuba, Sultan : Sudán, Syria : Siria, Pakistan : Pakistán, Palestine Palestina, Israel Israel, Iraq : Irak, Afghanistan : Afganistán, Libya : Libia, Turkey : Turquía, Thailand : Tailandia, Singapore : Singapur, South Africa : Sudáfrica, Mexico : México, Peru : Perú, Indonesia : Indonesia, GD Guangdong, FJ : Fujian, JL : Jilin, LN : Liaoning, TW : Taiwan (China), GZ : Guizhou, AH : Anhui, HL : Heilongjiang, HA : Henan, SC : Sichuan, HE : Hebei, YN : Yunnan, HB : Hubei, HI : Hainan, QH : Qinghai, HN : Hunan, JX : Jiangxi, SX : Shanxi, SN : Shaanxi, ZJ : Zhejiang, GS : Gansu, JS : Jiangsu, SD : Shandong, BJ : Beijing, SH : Shanghai, TJ : Tianjin, CQ : Chongqing, MO : Macao (China), HK : Hong Kong (China), NX : Ningxia, GX : Guangxi, XJ : Xinjiang, XZ : Tíbet, NM : Mongolia Interior
white	Sí	Integer	Acción protectora: \n - 0 : Block \n - 1 : Allow \n - 2 : Log only
description	No	String	Descripción de la regla

Parámetros de respuesta

Código de estado: 200

Tabla 4-274 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la regla.
policyid	String	ID de política
geoip	String	Códigos para regiones que se pueden utilizar en una regla de control de acceso de geolocalización. \n CN : China, AB2 : Fuera de China, AB : Fuera de China continental, Hong Kong, Macao y Taiwán, CA : Canadá, US : Estados Unidos, AU : Australia, IN : India, JP : Japón, UK : Reino Unido, FR : Francia, DE : Alemania, BR : Brasil, Ukraine : Ucrania, North Korea : Corea del Norte, The Republic of Korea : La República de Corea, Iran : Irán, Cuba : Cuba, Sultan : Sudán, Syria : Siria, Pakistan : Pakistán, Palestine : Palestina, Israel : Israel, Iraq : Irak, Afghanistan : Afganistán, Libya : Libia, Turkey : Turquía, Thailand : Tailandia, Singapore : Singapur, South Africa : Sudáfrica, Mexico : México, Peru : Perú, Indonesia : Indonesia, GD : Guangdong, FJ : Fujian, JL : Jilin, LN : Liaoning, TW : Taiwan (China), GZ : Guizhou, AH : Anhui, HL : Heilongjiang, HA : Henan, SC : Sichuan, HE : Hebei, YN : Yunnan, HB : Hubei, HI : Hainan, QH : Qinghai, HN : Hunan, JX : Jiangxi, SX : Shanxi, SN : Shaanxi, ZJ : Zhejiang, GS : Gansu, JS : Jiangsu, SD : Shandong, BJ : Beijing, SH : Shanghai, TJ : Tianjin, CQ : Chongqing, MO : Macao (China), HK : Hong Kong (China), NX : Ningxia, GX : Guangxi, XJ : Xinjiang, XZ : Tíbet, NM : Mongolia Interior
white	Integer	Acción protectora: \n - 0 : Block \n - 1 : Allow \n - 2 : Log only
timestamp	Long	Marca de tiempo de creación de reglas

Código de estado: 400

Tabla 4-275 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-276 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-277 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/geoip?
enterprise_project_id=0

{
  "white" : 0,
  "description" : "demo",
  "name" : "demo",
  "geoip" : "SH|Afghanistan"
}
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "02dafa406c4941368a1037b020f15a53",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650534513775,
  "description" : "demo",
  "status" : 1,
  "geoip" : "SH|Afghanistan",
  "white" : 0,
  "geoTagList" : [ "SH", "Afghanistan" ]
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.

Código de estado	Descripción
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.3.19 Actualización de una regla de control de acceso de geolocalización

Función

Esta API se utiliza para actualizar una regla de control de acceso de geolocalización.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/geoup/{rule_id}

Tabla 4-278 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy (valor del campo id en el cuerpo de la respuesta).
rule_id	Sí	String	ID de la regla. Se puede obtener llamando a la API ListGeoipRule . (el valor del campo id en el cuerpo de la respuesta)

Tabla 4-279 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-280 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-281 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
geoip	Sí	String	Códigos para regiones que se pueden utilizar en una regla de control de acceso de geolocalización. \n (CN:China AB2 : Fuera de China continental, AB : Fuera de China continental, Hong Kong, Macao y Taiwán, CA : Canadá, US .: Estados Unidos, AU : Australia, IN : India, JP : Japón, UK : Reino Unido, FR : Francia, DE : Alemania, BR : Brasil, Ucrania : Ucrania, North Korea : Corea del Norte, The Republic of Korea : Corea del Sur, Iran : Irán, Cuba : Cuba, Sultan : Sudán, Syria : Siria, Pakistan : Pakistán, Palestine , Israel Israel, Iraq : Irak, Afganistan : Afganistán, Libya : Libia, Turkey : Turquía, Tailandia : Tailandia, Singapore : Singapur, South Africa : Sudáfrica, Mexico : México, Peru : Perú, Indonesia : Indonesia, GD Guangdong, FJ : Fujian, JL : Jilin, LN : Liaoning, TW : Taiwán (China), GZ : Guizhou, AH : Anhui, HL : Heilongjiang, HA : Henan, SC : Sichuan, HE : Hebei, YN : Yunnan, HB : Hubei, HI : Hainan, QH : Qinghai, HN : Hunan, JX : Jiangxi, SX : Shanxi, SN : Shaanxi, ZJ : Zhejiang, GS : Gansu, JS : Jiangsu, SD : Shandong, BJ : Pekín, SH : Shanghai, TJ : Tianjin, CQ : Chongqing, MO : Macao (China) HK : Hong Kong (China), NX : Ningxia, GX : Guangxi, XJ : Xinjiang, XZ : Tibet, NM : Mongolia Interior
white	Sí	Integer	Acción protectora: \n - 0 : Block \n - 1 : Allow \n - 2 : Log only

Parámetros de respuesta

Código de estado: 200

Tabla 4-282 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la regla.
policyid	String	ID de política
geoip	String	Códigos para regiones que se pueden utilizar en una regla de control de acceso de geolocalización. \n (CN: China AB2 : Fuera de China continental, AB : Fuera de China continental, Hong Kong, Macao y Taiwán, CA : Canadá, US .: Estados Unidos, AU : Australia, IN : India, JP : Japón, UK : Reino Unido, FR : Francia, DE : Alemania, BR : Brasil, Ukraine : Ucrania, North Korea : Corea del Norte, The Republic of Korea : Corea del Sur, Iran : Irán, Cuba : Cuba, Sultan : Sudán, Syria : Siria, Pakistan : Pakistán, Palestine , Israel Israel, Iraq : Irak, Afganistan : Afganistán, Libya : Libia, Turkey : Turquía, Tailandia : Tailandia, Singapore : Singapur, South Africa : Sudáfrica, Mexico : México, Peru : Perú, Indonesia : Indonesia, GD Guangdong, FJ : Fujian, JL : Jilin, LN : Liaoning, TW : Taiwán (China), GZ : Guizhou, AH : Anhui, HL : Heilongjiang, HA : Henan, SC : Sichuan, HE : Hebei, YN : Yunnan, HB : Hubei, HI : Hainan, QH : Qinghai, HN : Hunan, JX : Jiangxi, SX : Shanxi, SN : Shaanxi, ZJ : Zhejiang, GS : Gansu, JS : Jiangsu, SD : Shandong, BJ : Pekín, SH : Shanghai, TJ : Tianjin, CQ : Chongqing, MO : Macao (China) HK : Hong Kong (China), NX : Ningxia, GX : Guangxi, XJ : Xinjiang, XZ : Tibet, NM : Mongolia Interior
white	Integer	Acción protectora: \n - 0 : Block \n - 1 : Allow \n - 2 : Log only

Código de estado: 400

Tabla 4-283 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-284 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-285 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}?
enterprise_project_id=0

{
  "white" : 0,
  "description" : "demo",
  "name" : "demo",
  "geoip" : "BJ|Afghanistan"
}
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "id" : "02dafa406c4941368a1037b020f15a53",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "description" : "demo",
  "geoip" : "BJ|Afghanistan",
  "white" : 0,
  "geoTagList" : [ "BJ", "Afghanistan" ]
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.

Código de estado	Descripción
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.3.20 Eliminación de una regla de control de acceso de geolocalización

Función

Esta API se utiliza para eliminar una regla de control de acceso de geolocalización.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}

Tabla 4-286 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .
rule_id	Sí	String	ID de la regla de control de acceso de geolocalización. Se puede obtener llamando a la API ListGeoipRule .

Tabla 4-287 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-288 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-289 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la regla.
policyid	String	ID de política

Parámetro	Tipo	Descripción
geoip	String	Códigos para regiones que se pueden utilizar en una regla de control de acceso de geolocalización. \n CN : China, AB2 : Fuera de China continental, AB : Fuera de China continental, Hong Kong, Macao y Taiwán, CA : Canadá, US : Estados Unidos, AU : Australia, IN : India, JP : Japón, UK : Reino Unido, FR : Francia, DE : Alemania, BR : Brasil, Ukraine : Ucrania, North Korea : Corea del Norte, The Republic of Korea : La República de Corea, Iran : Irán, Cuba : Cuba, Sultan : Sudán, Syria : Siria, Pakistan : Pakistan, Palestine : Palestina, Israel : Israel, Iraq : Irak, Afghanistan : Afganistán, Libya : Libia, Turkey : Turquía, Thailand : Tailandia, Singapore : Singapur, South Africa : Sudáfrica, Mexico : México, Peru : Perú, Indonesia : Indonesia, GD : Guangdong, FJ : Fujian, JL : Jilin, LN : Liaoning, TW : Taiwan (China), GZ : Guizhou, AH : Anhui, HL : Heilongjiang, HA : Henan, SC : Sichuan, HE : Hebei, YN : Yunnan, HB : Hubei, HI : Hainan, QH : Qinghai, HN : Hunan, JX : Jiangxi, SX : Shanxi, SN : Shaanxi, ZJ : Zhejiang, GS : Gansu, JS : Jiangsu, SD : Shandong, BJ : Beijing, SH : Shanghai, TJ : Tianjin, CQ : Chongqing, MO : Macao (China), HK : Hong Kong (China), NX : Ningxia, GX : Guangxi, XJ : Xinjiang, XZ : Tíbet, NM : Mongolia Interior
white	Integer	Acción protectora: \n - 0 : Block \n - 1 : Allow \n - 2 : Log only
description	String	Descripción.
timestamp	Long	Hora en que se crea la regla.

Código de estado: 400

Tabla 4-290 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-291 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-292 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "id" : "02dafa406c4941368a1037b020f15a53",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650534513775,
  "description" : "demo",
  "status" : 1,
  "geoip" : "BJ|Afghanistan",
  "white" : 0,
  "geoTagList" : [ "BJ", "Afghanistan" ]
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.3.21 Consulta de la lista de reglas de protección web contra manipulaciones

Función

Esta API se utiliza para consultar la lista de reglas de protección web contra manipulaciones.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/antitamper

Tabla 4-293 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Yes	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-294 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.
page	No	Integer	Número de página de los datos a devolver durante la consulta de paginación. El valor varía de 0 a 100000 . El valor predeterminado es 1 , que indica que se devuelven los datos de la primera página.
pagesize	No	Integer	Número de resultados en cada página durante la consulta de paginación. El valor varía de 1 a 100 . El valor predeterminado es 10 , lo que indica que cada página contiene 10 resultados.

Parámetros de solicitud

Tabla 4-295 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-296 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Cantidad de reglas
items	Array of AntiTamperRuleResponseBody objects	Reglas

Tabla 4-297 AntiTamperRuleResponseBody

Parámetro	Tipo	Descripción
id	String	ID de la regla.
policyid	String	ID de política
timestamp	Long	Tiempo.
description	String	Tiempo de creación de reglas.
status	Integer	Estado de la regla. El valor puede ser 0 (deshabilitado) o 1 (habilitado).
hostname	String	Nombre de dominio para la regla de protección antimanipulación
url	String	URL protegida por la regla de protección contra manipulaciones web

Código de estado: 400

Tabla 4-298 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-299 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-300 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "b77c3182957b46ed8f808a1998245cc4",
    "policyid" : "bdba8e224cbd4d11915f244c991d1720",
    "policyname" : "demo",
    "timestamp" : 1647499571037,
    "description" : "",
    "status" : 0,
    "hostname" : "www.demo.com",
    "url" : "/sdf"
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error del servidor interno

Códigos de error

Consulte [Códigos de error](#).

4.3.22 Creación de una regla de protección contra manipulaciones Web

Función

Esta API se utiliza para crear una regla de protección web contra manipulaciones.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/antitamper

Tabla 4-301 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Tabla 4-302 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-303 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-304 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
hostname	Sí	String	Sitio web protegido. Se puede obtener llamando a la API ListHost en modo cloud (valor del campo hostname en el cuerpo de la respuesta).
url	Yes	String	URL protegida por la regla de protección contra manipulaciones web. El valor debe estar en el formato de URL estándar, por ejemplo, /admin/xxx o /admin/. El asterisco (*) indica el prefijo de ruta.
description	No	String	Descripción de la regla

Parámetros de respuesta

Código de estado: 200

Tabla 4-305 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la regla.
policyid	String	ID de política
hostname	String	Nombre de dominio protegido por la regla de protección contra manipulaciones web

Parámetro	Tipo	Descripción
url	String	URL protegida por la regla de protección contra manipulaciones web
description	String	Tiempo de creación de reglas.
status	Integer	Estado de la regla. El valor puede ser 0 (deshabilitado) o 1 (habilitado).

Código de estado: 400

Tabla 4-306 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-307 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-308 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper?
enterprise_project_id=0

{
  "hostname" : "www.demo.com",
  "url" : "/test",
  "description" : "demo"
}
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "id" : "eed1c1e9c1b04b4bad4ba1186387a5d8",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "timestamp" : 1650594937397,
  "description" : "demo",
  "status" : 1,
  "hostname" : "www.demo.com",
  "url" : "/test"
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error del servidor interno

Códigos de error

Consulte [Códigos de error](#).

4.3.23 Eliminación de una regla de protección contra manipulaciones web

Función

Esta API se utiliza para eliminar una regla de protección de manipulación web.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}

Tabla 4-309 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
policy_id	Sí	String	ID de política. Se puede obtener llamando a la API ListPolicy .

Parámetro	Obligatorio	Tipo	Descripción
rule_id	Sí	String	ID de la regla antimanipulación. Se puede obtener llamando a la API ListAntitamperRule .

Tabla 4-310 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-311 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-312 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de la regla.
policyid	String	ID de política
url	String	URL protegida por la regla de protección contra manipulaciones web
timestamp	Long	Marca de tiempo de creación de reglas

Código de estado: 400

Tabla 4-313 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-314 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-315 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}?enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

La solicitud se ha realizado correctamente.

```
{
  "total" : 1,
  "items" : [ {
    "id" : "b77c3182957b46ed8f808a1998245cc4",
    "policyid" : "bdba8e224cbd4d11915f244c991d1720",
    "policyname" : "demo",
    "timestamp" : 1647499571037,
    "description" : "",
    "status" : 0,
    "hostname" : "www.demo.com",
    "url" : "/sdf"
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	La solicitud se ha realizado correctamente.
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.4 Certificate Management

4.4.1 Aplicación de un certificado a un nombre de dominio

Función

Esta API se utiliza para aplicar un certificado a un nombre de dominio.

URI

POST /v1/{project_id}/waf/certificate/{certificate_id}/apply-to-hosts

Tabla 4-316 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
certificate_id	Sí	String	ID de certificado HTTPS. Se puede obtener llamando a la API ListCertificates .

Tabla 4-317 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-318 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-319 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
cloud_host_ids	No	Array of strings	ID del nombre de dominio HTTPS en modo nube. Se puede obtener llamando a la API ListHost .
premium_host_ids	No	Array of strings	ID del nombre de dominio HTTPS en modo dedicado. Se puede obtener llamando a la API ListPremiumHost .

Parámetros de respuesta

Código de estado: 200

Tabla 4-320 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID del certificado.
name	String	Nombre del certificado
timestamp	Long	Tiempo.
expire_time	Long	Fecha de expiración
bind_host	Array of CertificateBindingHostBody objects	Lista de nombres de dominios

Tabla 4-321 CertificateBundingHostBody

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio
waf_type	String	Modo WAF. El valor puede ser cloud para el modo cloud o premium para el modo dedicado. Valores de enumeración: <ul style="list-style-type: none"> ● cloud ● premium

Código de estado: 400

Tabla 4-322 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-323 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-324 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}/apply-to-hosts?enterprise_project_id=0
```

```
{
  "cloud_host_ids" : [ "85e554189d494c0f97789e93531c9f90" ],
  "premium_host_ids" : [ "4e9e97c425fc463c8f374b90124e8392" ]
}
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "3ac1402300374a63a05be68c641e92c8",
  "name" : "www.abc.com",
  "timestamp" : 1636343349139,
  "expire_time" : 1650794100000,
  "bind_host" : [ {
    "id" : "e350cf556da34adab1f017523d1c05ed",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud",
    "bandwidth" : 0,
    "qps" : 0
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.4.2 Consulta de la lista de certificados

Función

Esta API se utiliza para consultar la lista de certificados.

URI

GET /v1/{project_id}/waf/certificate

Tabla 4-325 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-326 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.
page	No	Integer	Número de página de los datos a devolver durante la consulta de paginación. El valor varía de 0 a 100000 . El valor predeterminado es 1 , que indica que se devuelven los datos de la primera página. Predeterminado: 1
pagesize	No	Integer	Número de resultados en cada página durante la consulta de paginación. El valor varía de 1 a 100 . El valor predeterminado es 10 , lo que indica que cada página contiene 10 resultados. Predeterminado: 10
name	No	String	Nombre del certificado
host	No	Boolean	Si se desea obtener el nombre de dominio para el que se utiliza el certificado. El valor predeterminado es false . \n -true : Obtener los certificados que se han utilizado para los nombres de dominio. \n -false : obtenga los certificados que no se utilizan para ningún nombre de dominio. Predeterminado: false
exp_status	No	Integer	Estado del certificado. Las opciones son 0 , 1 y 2 . 0 : El certificado es válido. 1 : El certificado ha caducado; 2 : El certificado caducará en el plazo de un mes.

Parámetros de solicitud

Tabla 4-327 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-328 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
items	Array of CertificateBody objects	Certificados
total	Integer	Número total de certificados

Tabla 4-329 CertificateBody

Parámetro	Tipo	Descripción
id	String	ID de certificado
name	String	Nombre del certificado
content	String	Archivo de certificado, que está en formato PEM.
key	String	Clave privada del certificado, que está en formato PEM.
expire_time	Long	Marca de tiempo de caducidad del certificado.
exp_status	Integer	Estado del certificado. Las opciones son 0 , 1 y 2 . 0 : El certificado es válido. 1 : El certificado ha caducado; 2 : El certificado caducará en el plazo de un mes.
timestamp	Long	Marca de tiempo de carga de certificado.

Parámetro	Tipo	Descripción
bind_host	Array of BindHost objects	Nombre de dominio asociado al certificado

Tabla 4-330 BindHost

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio
waf_type	String	Modo de nombre de dominio: cloud (modo de cloud) / premium (modo dedicado)
mode	String	Este parámetro es requerido solamente por el modo dedicado.

Código de estado: 400

Tabla 4-331 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-332 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-333 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error

Parámetro	Tipo	Descripción
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/certificate?enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "dc443ca4f29c4f7e8d4adaf485be317b",
    "name" : "demo",
    "timestamp" : 1643181401751,
    "expire_time" : 1650794100000,
    "bind_host" : [ ],
    "exp_status" : 2
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.4.3 Creación de un certificado

Función

Esta API se utiliza para crear un certificado.

URI

POST /v1/{project_id}/waf/certificate

Tabla 4-334 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-335 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-336 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-337 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
name	Sí	String	Nombre del certificado. El valor puede contener un máximo de 64 caracteres. Solo se permiten dígitos, letras, guiones (-) guiones bajos y puntos (.).
content	Sí	String	Archivo de certificado. Sólo se admiten certificados y archivos de clave privada en formato PEM, y los caracteres de nueva línea del archivo deben reemplazarse por \n.

Parámetro	Obligatorio	Tipo	Descripción
key	Sí	String	Certificación de clave privada. Sólo se admiten certificados y archivos de clave privada en formato PEM, y los caracteres de nueva línea de los archivos deben reemplazarse por \n.

Parámetros de respuesta

Código de estado: 200

Tabla 4-338 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de certificado
name	String	Nombre del certificado
content	String	Archivo de certificado en formato PEM
key	String	Clave privada del certificado, que está en formato PEM.
expire_time	Long	Marca de tiempo de caducidad del certificado
exp_status	Integer	Estado de caducidad del certificado. Las opciones son 0 , 1 y 2 . 0 : El certificado es válido. 1 : El certificado ha caducado; 2 : El certificado caducará en el plazo de un mes.
timestamp	Long	Marca de tiempo de carga de certificado
bind_host	Array of BindHost objects	Nombre de dominio asociado al certificado

Tabla 4-339 BindHost

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio
waf_type	String	Modo de nombre de dominio: cloud (modo de cloud) / premium (modo dedicado)
mode	String	Este parámetro es requerido solamente por el modo dedicado.

Código de estado: 400

Tabla 4-340 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-341 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-342 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
POST https://{Endpoint}/v1/{project_id}/waf/certificate?enterprise_project_id=0
{
  "name" : "demo",
  "content" : "-----BEGIN CERTIFICATE-----
MIIDyzCCArOgAwIBAgIJAN5U0Z4Bh5ccMA0GCSqGSIb3DQEBCwUAMHwxCzAJBgNV
BAYTA1pIMRIwEAYDVQQIDAlHVUFOR0RPTkcxETAPBgNVBACMCCERPTkdHVUFOMQ0w
CwYDVQQKDARERURuTFMQswCQYDVQQQLDAJESzELMAkGA1UEAwwCT0QxHTAbBgkqhkiG
9w00BCQEWDk8IZC5odWF3ZlZlY29tMB4XDTEyMTE4MTE4MTk0MVoXDTEyMTE4MTE4
MTk0MVoWfDDELMAkGA1UEBhMCWkgxZjAQBgNVBAGMUCdVQU5HRE90RzERMA8GA1UE
BwwIRE90R0dVQU4xDTALBgNVBAoMBERFS0UxZzAJBgNVBAsMAkRMLMQswCQYDVQQD
DAJPRDEdMBsGCSqGSIb3DQEJARYOTWhkLmhlYXdlYXN5b20wggeiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDcoLfk62//r0RHfyweYBj97S4NsJ8Qj0RG+Y02
OgwhQmRiNnJubJwP8Nqgyd86zr+fsSQxKBaBCosn1PcN2Pj2vPJD6NEk4I6VdOwr /
kFYm1OcimhSfW4wt6VakniOKIYGrCxxvQe1X2OyBxT+ocTLRgEIB8ZbvJyPNseg
feLEUuPYRqQ5kXLgJH2/3NwZF0gBHvV/b0714fR+sWJMnIA2yIjSBQ0DEAOSusXo FQ/
WRbBRH7DrQmxGiXsq4VELEr9Nnc/Kywq+9pYi8L+mKeRL+lcmMbxXC/3k60fMB
tVTiwcmS1Mkr3iG03i8u6H7RSvRwyBz9G9se+tmJZTPH61YtAgMBAAGjUDBOMB0G
A1UdDgQWBBQprUUFxW+gIkpzXdrYlswJfSahWjAfBgNVHSMEGDAWgBQprUUFxW+g
IkpzXdrYlswJfSahWjAMBGNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQA2
603KozsQoIkeLvqDJlcAxwWRfnW8Sv1aSJaulhHgneMt9bQgIL+3PJWA/iMniOhU o/
kVwkiUicxw4t7RwP0hVms0OZw59MuqKd3oCSWkYO4vEHS3t40JDWnGDnmQ4sol
RkOWJwL4w8tnPe3qY9JSupjlsu6Y1hlvKtEfn2vEKFNsuMhidkUpUAJWodHhWBQH
```

```
wgIDo4/6yTnWZNGK8JDa186Dm5IchXealEoYBJSxHxiJb7HeWQlkre+MCYi1RHoin 4mIXTr0oT4/
jWlglk1Sz6/ZhGRq+7W7tI17cvzCe+4XsVZienAcYoNd/WLfo91PD4 yAsRrXOjWlso1Bj0BkDz -----
END CERTIFICATE-----",
"key" : "-----BEGIN PRIVATE KEY-----
MIIEVwIBADANBgkqhkiG9w0BAQEFAASCBAkkgwS1AgEAAoIBAQDcoLfk62//r0RH
FyweYBj97S4NsJ8QjORG+Y02OgwhQmRiNNjubJwP8Nqqyd86zr+fsSQxKBaBCosn
lPcN2Pj2vPJD6NEk4I6VdOWr/kFYML0cimhSfW4wt6VakniOKIYGrCxxvQe1X2Oy BxT
+ocTLRgEIB8ZbvJyPNsegfeLEUuPYRpQ5kXLgJH2/3NwZFOgBHVv/b0714fR+
sWJMnIA2yIjSBQ0DEAOSusXoFQ/WRbBRH7DrQmxGiXsq4VELEr9Nnc/Kywq+9pYi 8L+mKeRL+lcmMbXC/
3k60fMBtVTiwcmS1Mkr3iG03i8u6H7RSvRwyBz9G9se+tmJ ZTPH61YtAgMBAACggEBAL+xZxm/QoqXT
+2stoqV2GEYaMFASpRqxlocjZMmEE/9 jZa
+cBWIjHhVpsjRqYfBDCHEebu0JwlrjcjIavgnIvnO5XgXm1A9Q+WbscokmcX1 xCvpHgc+MDVn
+uWdCd4KW5kEk4EnSsFN5iNsf+1VxNURN+gwSSp/0E+muwA5IISO G6HQ+p6qs52JAitX5t/
7ruKoHYXJxBnf7TUs7768qrh++KPKpPlq044qoYlCGOln 4urPBHuNly04GgGw
+vkaqjqQovZrNLVOMMaFWBxsDWBehgSSBQTj+f3NCxneGYtt8 3SCTZQI5nIkb+r/
M455EwKTSXuEsNHoIwx7L6GEPBQECgYEA8IxgK2fYykloICoh
TFJaRavYjyKa2+Aza4qT9SGY9Y30VPClPjBB1vUu5M9KrFuFz1v06nGEchmpEwOe
8vbRu7nLAQTGYfi8VK63q8w6F1FdAyCG6Sx+BWCfWxJzXsZLAJTFk1wi8HsOSlqh
6QNv0xbE2fLjXKf8MHvtrufip40CgYEA6sy87eDrkVgtq4ythAik3i1C5Z3v0fvx
mTb1G52Z210yocNq3Tf/blZwoIc1ik6cyBzY6z1bIrbSzArCqm0sb2iD+kJL8100 /
qqdXjBxZUkKiVAMNnp7xJGZHHFKWuXT2+UX/tlyx4tT4dzrF1kdXkcMmqfsRxd
lNEVaAaT8SECyAoU7BtpIun43YtpUfr3pSIN6ozeKoxSbw9i4MNC+4fSDRPC+ 80ImcmZRL7taF
+Y7p0jxAOTuIkdJC8NbAiv5J9WzrwQ+5MF2BPB/2bYnRa6tNoFH kZDy/
9bXys16qw2p5Ety8wVcgZTMvFMG1G/32IpZ65FYWEU8L5qSRwfFhQKBgQC9 ihjZTj/
bTHtRiHZppzCvyYm/Igd+Uwtsy0uXR1n0G1SQENgrTBD/J6AzdFJae6te P0U8YIM50qxf2i/as9ay
+IPRecM14eSxz7jJWAGx6Yx/3AZ+hAB1ZbNbqniCLYNk d0MvjwmA25ATO+ro40Z7AdEpQbk319aG/
WFyYBz9AQKBgQCucFPA115es1L8196V Wmr2Qo0tqz17CGSoWQk2Sa2HZtzdfofXAaaqo
+zvJ6RPHtJh0jgJtx536DvV3egI 37YrdQyJbCPZXQ3SPggqWCorUnXBwq/
nxS06uwu6JBxUfc57ijmMU4fWYNrvkkmWb 7keAg/r5Uy1j0MAvBN1I6lB8pg== -----END PRIVATE
KEY-----"
}
```

Ejemplo de respuestas

Ninguno

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.4.4 Consulta de un certificado

Función

Esta API se utiliza para consultar un certificado.

URI

GET /v1/{project_id}/waf/certificate/{certificate_id}

Tabla 4-343 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
certificate_id	Sí	String	ID de certificado HTTPS. Se puede obtener llamando a la API ListCertificates .

Tabla 4-344 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-345 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-346 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID del certificado.

Parámetro	Tipo	Descripción
name	String	Nombre del certificado
content	String	Archivo de certificado, que está en formato PEM.
key	String	Clave privada del certificado, que está en formato PEM.
expire_time	Long	Marca de tiempo de caducidad del certificado
exp_status	Integer	Estado del certificado. Las opciones son 0 , 1 y 2 . 0 : El certificado es válido. 1 : El certificado ha caducado; 2 : El certificado caducará en el plazo de un mes.
timestamp	Long	Marca de tiempo de carga de certificado
bind_host	Array of BindHost objects	Nombre de dominio asociado al certificado

Tabla 4-347 BindHost

Parámetro	Tipo	Descripción
Identificación	String	ID de nombre de dominio
hostname	String	Nombre de dominio
waf_type	String	Modo de nombre de dominio: cloud (modo de cloud) / premium (modo dedicado)
mode	String	Este parámetro es requerido solamente por el modo dedicado.

Código de estado: 400

Tabla 4-348 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-349 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-350 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "6e2be127b79f4a418414952ad5d8c59f",
  "name" : "certificatename94319",
  "content" : "-----BEGIN CERTIFICATE-----\nMIIB
+TCCAAoGAWIBAgIUJP9I8OupQ77w0bGL2yWOQXreM4kwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMCQV
UxEzARBgNVBAGMC1NvbWUtU3RhdGUxLzANBgNVBAoMBkh1YXdlTEcMBoGA1UEAwTd2FmLmhl1YXdlaWNs
b3VklmNvbTAEFw0yMDA3MDkwNTQ2MDRaFw0yMDA4MDgwNTQ2MDRaMFExCzAJBgNVBAYTAkFVMRMwEQYDVQ
QIDApTb211LVN0YXR1MQ8wDQYDVQQKDAZIdWF3ZWkxHDAaBgNVBAMME3dhZi5odWF3ZWljbG91ZC5jb20w
XDANBgkqhkiG9w0BAQEFAANLADBIAkEA0UEbMzbvgoJTKrKcDUw9xjFqxM7BaQFM3SLsQlmd5hkzygyL1r
a
+cWajPJlTCxz9Ph6qldna2+OrIuTdvCcpjwIDAQABo1MwUTAdBgNVHQ4EFgQUE7ZQNcg13lmryx1s5gy9m
nClrsYwHwYDVR0jBBgwFoAUE7ZQNcg13lmryx1s5gy9mnClrsYwDwYDVR0TAQH/BAUwAwEB/
zANBgkqhkiG9w0BAQsFAANBAM5wGi88jYWLgOnGbae5hH3I9lMBKxGqv17Cbm1tjWuUogVINz861qvCpuh
+ei2lqZqHaczqdUNQxMh54yot9F2yVWjwIhANS1Y1Jv89WEU/
ZvvMS9a4638Msv2c4GGp08RtXNYn0BAiA0H4b+cwoEbZjHf+HYg6Fo
+uxu5TvSaw8287a6Qo0LyQIfvZS1YYWp1T6oiX5rdLzBiap4N0gJWdsa2ihmV59LAQIqK8N
+j1daq63b0bJ9k4HruhQtpgxI6U9nFBemH4zTRYM=\n-----END RSA PRIVATE KEY-----\n",
  "timestamp" : 1650595334578,
  "expire_time" : 1596865564000,
  "bind_host" : [ {
    "id" : "978b411657624c2db069cd5484195d1c",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud"
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.4.5 Eliminación de un certificado.

Función

Esta API se utiliza para eliminar un certificado.

URI

DELETE /v1/{project_id}/waf/certificate/{certificate_id}

Tabla 4-351 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
certificate_id	Sí	String	ID de certificado HTTPS. Se puede obtener llamando a la API de ListCertificates .

Tabla 4-352 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-353 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-354 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de certificado
name	String	Nombre del certificado
content	String	Archivo de certificado, que está en formato PEM.
key	String	Clave privada del certificado, que está en formato PEM.
expire_time	Long	Marca de tiempo de caducidad del certificado
exp_status	Integer	Estado del certificado. Las opciones son 0 , 1 y 2 . 0 : El certificado es válido. 1 : El certificado ha caducado; 2 : El certificado caducará en el plazo de un mes.
timestamp	Long	Marca de tiempo de carga de certificado
bind_host	Array of BindHost objects	Nombre de dominio asociado al certificado

Tabla 4-355 BindHost

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio

Parámetro	Tipo	Descripción
waf_type	String	Modo de nombre de dominio: nube (modo nube) / premium (modo dedicado)
mode	String	Este parámetro es requerido solamente por el modo dedicado.

Código de estado: 400

Tabla 4-356 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-357 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-358 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
DELETE https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "e1d87ba2d88d4ee4a3b0c829e935e5e0",
  "name" : "certificatename29556",
  "timestamp" : 1650594410630,
  "expire_time" : 1596865564000
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.4.6 Modificación de un certificado

Función

Esta API se utiliza para modificar un certificado.

URI

PUT /v1/{project_id}/waf/certificate/{certificate_id}

Tabla 4-359 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
certificate_id	Sí	String	ID de certificado HTTPS. Se puede obtener llamando a la API ListCertificates .

Tabla 4-360 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-361 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Tabla 4-362 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
name	No	String	Nombre del certificado. El valor puede contener un máximo de 64 caracteres. Solo se permiten dígitos, letras, guiones (-) guiones bajos y puntos (.).

Parámetros de respuesta

Código de estado: 200

Tabla 4-363 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de certificado
name	String	Nombre del certificado
expire_time	Long	Marca de tiempo cuando caduca el certificado
timestamp	Long	Tiempo.

Código de estado: 400

Tabla 4-364 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-365 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-366 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
PUT https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}?
enterprise_project_id=0

{
  "name" : "demo"
}
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "360f992501a64de0a65c50a64d1ca7b3",
  "name" : "demo",
  "timestamp" : 1650593797892,
  "expire_time" : 1596865564000
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.5 Gestión de Eventos

4.5.1 Esta API se utiliza para consultar la lista de eventos de ataque.

Función

Esta API se utiliza para consultar la lista de eventos de ataque. Actualmente, esta API no admite consultas de todos los eventos de protección. El parámetro **pagesize** no se puede establecer en **-1**. Cuanto mayor sea el volumen de datos, mayor será el consumo de memoria. Se puede consultar un máximo de 10,000 de registros de datos. Por ejemplo, si el número de registros de datos en un periodo definido por el usuario excede de 10,000 no se pueden consultar los datos cuya página es 101 (o **pagesize** es mayor que 100). Debe ajustar el intervalo de tiempo a un período más largo y luego consultar los datos.

URI

GET /v1/{project_id}/waf/event

Tabla 4-367 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-368 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.
recent	No	String	Rango de tiempo para consultar registros. Este parámetro no se puede usar junto con el parámetro from o to . Valores de enumeración: <ul style="list-style-type: none"> ● yesterday ● today ● 3days ● 1week ● 1month
attacks	No	Array	Tipo de ataque \n - vuln : Otros tipos de ataque\n - sqli : ataque de inyección SQL\n - lfi : archivo local contiene\n - cmdi : ataque de inyección de comando\n - xss : ataque XSS\n - robot : rastreador malicioso\n - rfi : archivo remoto contiene\n - custom_custom : protección de precisión\n - cc : ataque cc\n - webshell : troyano de sitio web\n - custom_whiteblackip : bloqueo de lista de bloqueo y lista de confianza\n - custom_geoiip : control de acceso geográfico\n - antiamper : antimanipulación\n - antiticrawler : antimanipulación\n - leakage : antimanipulación de información del sitio web\n - illegal : solicitudes ilegalesç
from	No	Long	Hora de inicio (marca de tiempo de 13 dígitos). Este parámetro debe usarse junto con to , pero no puede usarse junto con recent .
to	No	Long	Hora de finalización (marca de tiempo de 13 dígitos). Este parámetro debe usarse junto con from , pero no puede usarse junto con recent .

Parámetro	Obligatorio	Tipo	Descripción
hosts	No	Array	ID de nombre de dominio. Se puede obtener llamando a la API ListHost .
page	No	Integer	Número de página de los datos a devolver durante la consulta de paginación. El valor varía de 0 a 100000 . El valor predeterminado es 1 , que indica que se devuelven los datos de la primera página.
pagesize	No	Integer	Número de resultados en cada página durante la consulta de paginación. El valor varía de 1 a 100 . El valor predeterminado es 10 , lo que indica que cada página contiene 10 resultados.

Parámetros de solicitud

Tabla 4-369 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-370 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Consultar el número de eventos de ataque
items	Array of ListEventItems objects	Esta API se utiliza para consultar los detalles sobre un evento de ataque.

Tabla 4-371 ListEventItems

Parámetro	Tipo	Descripción
id	String	ID del evento
time	Long	Ocurrencias
policyid	String	ID de política
sip	String	Dirección IP de origen
host	String	Nombre de dominio
url	String	URL atacada
attack	String	Tipo de ataque \n - vuln : Otros tipos de ataque\n - sqli : ataque de inyección SQL\n - lfi : archivo local contiene\n - cmdi : ataque de inyección de comando\n - xss : ataque XSS\n - robot : rastreador malicioso\n - rfi : archivo remoto contiene\n - custom_custom : protección de precisión\n - webshell : Trojan del sitio web\n - custom_whiteblackip : bloqueo de lista de bloques y lista de confianza\n - custom_geoip : bloqueo de control de acceso geográfico\n - antitamper : antimanipulación\n - anticrawler : antimanipulación\n - leakage : información del sitio web prevención de fugas\n - illegal : solicitudes ilegales
rule	String	ID de la regla coincidente
payload	String	Carga útil de hit
action	String	Acción protectora
request_line	String	Método y ruta de solicitud
headers	Object	Encabezado de solicitudes HTTP
cookie	String	Solicitar una cookie
status	String	Estado del código de respuesta
process_time	Integer	Tiempo de procesamiento
region	String	Localización
host_id	String	ID de nombre de dominio
response_time	Long	Tiempo de respuesta
response_size	Integer	Tamaño del cuerpo de la respuesta
response_body	String	Cuerpo de respuesta
request_body	String	Cuerpo

Código de estado: 400

Tabla 4-372 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-373 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-374 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
DELETE https://{Endpoint}/v1/{project_id}/waf/event?
enterprise_project_id=0&page=1&pagesize=10&recent=today
```

Ejemplo de respuestas

Código de estado: 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "04-0000-0000-0000-21120220421152601-2f7a5ceb",
    "time" : 1650525961000,
    "policyid" : "25f1d179896e4e3d87ceac0598f48d00",
    "host" : "x.x.x.x:xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "url" : "/osclass/oc-admin/index.php",
    "attack" : "lfi",
    "rule" : "040002",
    "payload" : " file=../../../../../../../../../../../../etc/passwd",
    "payload_location" : "params",
```

```

"sip" : "x.x.x.x",
"action" : "block",
"request_line" : "GET /osclass/oc-admin/index.php?
page=appearance&action=render&file=../../../../../../../../../../../../etc/passwd",
"headers" : {
  "accept-language" : "en",
  "ls-id" : "xxxxxx-xxxxxx-xxxx-xxxx-9c302cb7c54a",
  "host" : "x.x.x.x",
  "lb-id" : "2f5f15ce-08f4-4df0-9899-ec0cc1fcdc52",
  "accept-encoding" : "gzip",
  "accept" : "*/*",
  "user-agent" : "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/35.0.2309.372 Safari/537.36"
},
"cookie" : "HWWAFSESID=2a1d773f9199d40a53; HWWAFSESTIME=1650525961805",
"status" : "418",
"host_id" : "6fbe595e7b874dbbb1505da3e8579b54",
"response_time" : 0,
"response_size" : 3318,
"response_body" : "",
"process_time" : 2,
"request_body" : "{}"
} ]
}

```

Códigos de estado

Código de estado	Descripción
200	ok
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.5.2 Esta API se utiliza para consultar detalles de eventos de ataque.

Función

Consulta de detalles de un evento

URI

GET /v1/{project_id}/waf/event/{eventid}

Tabla 4-375 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
eventid	Sí	String	ID de evento. Se puede obtener llamando a la API ListEvent .

Tabla 4-376 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-377 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-378 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Número de eventos de ataque
items	Array of ShowEventItems objects	Esta API se utiliza para consultar los detalles sobre un evento de ataque.

Tabla 4-379 ShowEventItems

Parámetro	Tipo	Descripción
time	Long	Marca de tiempo cuando se produce el ataque, en milisegundos.
policyid	String	ID de política
sip	String	Dirección IP de origen
host	String	Nombre de dominio
url	String	URL atacada
attack	String	Tipo de ataque
rule	String	ID de la regla de hit
action	String	Protección
cookie	String	Cookie de la solicitud de ataque
headers	Object	Encabezado de la solicitud de ataque
host_id	String	ID del nombre de dominio atacado
id	String	ID de evento de protección
payload	String	Carga maliciosa
payload_location	String	Carga maliciosa
region	String	Ubicación geográfica de la dirección IP de origen
process_time	Integer	Tiempo de procesamiento
request_line	String	Cuerpo de la solicitud de ataque
response_size	Integer	Tamaño del cuerpo de la respuesta (byte)
response_time	Long	Tiempo de respuesta (ms)
status	String	Código de respuesta
request_body	String	Cuerpo

Código de estado: 400

Tabla 4-380 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-381 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-382 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
DELETE https://{Endpoint}/v1/{project_id}/waf/event{event_id}?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "09-0000-0000-0000-12120220421093806-a60a6166",
    "time" : 1650505086000,
    "policyid" : "173ed802272a4b0798049d7edffeff03",
    "host" : "x.x.x.x:xxxxxx-xxx-xxx-xxx-xxxxxxxxxx",
    "url" : "/mobile/DBconfigReader.jsp",
    "attack" : "vuln",
    "rule" : "091004",
    "payload" : " /mobile/dbconfigreader.jsp",
    "payload_location" : "uri",
    "sip" : "x.x.x.x",
    "action" : "block",
    "request_line" : "GET /mobile/DBconfigReader.jsp",
    "headers" : {
      "ls-id" : "c0d957e6-26a8-4f2e-8216-7fc9332a250f",
      "host" : "x.x.x.x:81",
      "lb-id" : "68d3c435-2607-45e0-a5e2-38980544dd45",
      "accept-encoding" : "gzip",
      "user-agent" : "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101
CSIRTx/2022"
    },
    "cookie" : "HWWAFSESID=2a0bf76a111c93926d; HWWAFSESTIME=1650505086260",
    "status" : "418",
    "region" : "Reserved IP",
    "host_id" : "e093a352fd3a4ddd994c585e2e1dda59",
```

```
"response_time" : 0,  
"response_size" : 3318,  
"response_body" : "",  
"process_time" : 0,  
"request_body" : "{}"  
} ]  
}
```

Códigos de estado

Código de estado	Descripción
200	ok
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.6 Panel de control

4.6.1 Consulta de estadísticas de solicitud de sitio web

Función

Esta API se utiliza para consultar las estadísticas de solicitud del sitio web.

URI

GET /v1/{project_id}/waf/overviews/statistics

Tabla 4-383 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-384 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.
from	Sí	Long	Hora de inicio (marca de tiempo de 13 dígitos). Este parámetro debe usarse junto con to .
to	Sí	Long	Hora de finalización (marca de tiempo de 13 dígitos). Este parámetro debe usarse junto con from .
hosts	No	String	Lista de los nombres de dominio a consultar
instances	No	String	Lista de instancias a consultar

Parámetros de solicitud

Tabla 4-385 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-386 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
[items]	Array of CountItem objects	Estadísticas de seguridad

Tabla 4-387 CountItem

Parámetro	Tipo	Descripción
key	String	Tipo
num	Integer	Cantidad

Código de estado: 400

Tabla 4-388 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-389 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 403

Tabla 4-390 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-391 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/statistics?
enterprise_project_id=0&from=1650470400196&to=1650522936196
```

Ejemplo de respuestas

Código de estado: 200

Operación exitosa.

```
[ {
  "key" : "ACCESS",
  "num" : 1190
}, {
  "key" : "PRECISE",
  "num" : 0
}, {
  "key" : "CRAWLER",
  "num" : 10
}, {
  "key" : "WEB_ATTACK",
  "num" : 22
}, {
  "key" : "CC",
  "num" : 0
}, {
  "key" : "ATTACK",
  "num" : 32
} ]
```

Códigos de estado

Código de estado	Descripción
200	Operación exitosa.
400	Error de solicitud.
401	Permisos de token insuficientes.
403	La cuota de recursos es insuficiente.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.6.2 Consulta de las estadísticas de QPS

Función

Esta API se utiliza para consultar las estadísticas de QPS.

URI

```
GET /v1/{project_id}/waf/overviews/qps/timeline
```

Tabla 4-392 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-393 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener llamando a la API ListEnterpriseProject de EPS.
from	Sí	Long	Hora de inicio (marca de tiempo de 13 dígitos en milisegundos). Este parámetro debe usarse junto con to .
to	Sí	Long	Hora de finalización (marca de tiempo de 13 dígitos en milisegundos). Este parámetro debe usarse junto con from .
hosts	No	String	ID de nombre de dominio, que se puede obtener llamando a la API ListHost
instances	No	String	ID de la instancia de WAF dedicada. Este parámetro solo se requiere para el modo WAF basado en instancias.
group_by	No	String	Dimensión de visualización. Por ejemplo, el valor es DAY si los datos se muestran por día.

Parámetros de solicitud

Tabla 4-394 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-395 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
[items]	Array of StatisticsTimelineItem objects	Cronología de las estadísticas de seguridad

Tabla 4-396 StatisticsTimelineItem

Parámetro	Tipo	Descripción
key	String	valor clave
timeline	Array of TimeLineItem objects	Cronología correspondiente al valor de clave

Tabla 4-397 TimeLineItem

Parámetro	Tipo	Descripción
time	Long	Tiempo
num	Integer	Cantidad

Código de estado: 400

Tabla 4-398 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-399 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error

Parámetro	Tipo	Descripción
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-400 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/qps/timeline?
enterprise_project_id=0&from=1650470400196&to=1650522936196
```

Ejemplo de respuestas

Código de estado: 200

ok

```
[ {
  "key" : "ACCESS",
  "timeline" : [ {
    "time" : 1650470400000,
    "num" : 0
  } ]
}, {
  "key" : "PRECISE",
  "timeline" : [ {
    "time" : 1650470400000,
    "num" : 0
  } ]
}, {
  "key" : "CRAWLER",
  "timeline" : [ {
    "time" : 1650470400000,
    "num" : 0
  } ]
}, {
  "key" : "CC",
  "timeline" : [ {
    "time" : 1650470400000,
    "num" : 0
  } ]
}, {
  "key" : "TOTAL_ATTACK",
  "timeline" : [ {
    "time" : 1650470400000,
    "num" : 0
  } ]
}, {
  "key" : "WEB_ATTACK",
  "timeline" : [ {
    "time" : 1650470400000,
```

```
"num" : 0
} ]
} ]
```

Códigos de estado

Código de estado	Descripción
200	ok
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.6.3 Consulta de estadísticas de uso de ancho de banda

Función

Consulta de estadísticas de uso de ancho de banda

URI

GET /v1/{project_id}/waf/overviews/bandwidth/timeline

Tabla 4-401 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-402 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API <code>ListEnterpriseProject</code> de EPS.
from	Sí	Long	Hora de inicio (marca de tiempo de 13 dígitos en milisegundos). Este parámetro debe usarse junto con <code>to</code> .

Parámetro	Obligatorio	Tipo	Descripción
to	Sí	Long	Hora de finalización (marca de tiempo de 13 dígitos en milisegundos). Este parámetro debe usarse junto con from .
hosts	No	String	Lista de nombres de dominio a consultar, que se puede obtener llamando a la API** ListHost
instances	No	String	Lista de instancia a consultar (solo para el modo de instanciación).
group_by	No	String	Dimensión de visualización. Por ejemplo, el valor es DAY si los datos se muestran por día.

Parámetros de solicitud

Tabla 4-403 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-404 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
[items]	Array of StatisticsTimelineItem objects	Cronología de las estadísticas de seguridad

Tabla 4-405 StatisticsTimelineItem

Parámetro	Tipo	Descripción
key	String	valor clave
timeline	Array of TimeLineItem objects	Cronología correspondiente al valor de clave

Tabla 4-406 TimeLineItem

Parámetro	Tipo	Descripción
time	Long	Tiempo
num	Integer	Cantidad

Código de estado: 400

Tabla 4-407 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-408 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-409 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/bandwidth/timeline?
enterprise_project_id=0&from=1650470400196&to=1650522936196
```

Ejemplo de respuestas

Código de estado: 200

ok

```
[ {
  "key" : "IN_BANDWIDTH",
  "timeline" : [ {
    "time" : 1650470400000,
    "num" : 0
  } ]
}, {
  "key" : "OUT_BANDWIDTH",
  "timeline" : [ {
    "time" : 1650470400000,
    "num" : 0
  } ]
}, {
  "key" : "BANDWIDTH",
  "timeline" : [ {
    "time" : 1650470400000,
    "num" : 0
  } ]
} ]
```

Códigos de estado

Código de estado	Descripción
200	ok
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.6.4 Consulta del número de solicitudes anormales

Función

Esta API se demanda para consultar el número de solicitudes anormales.

URI

```
GET /v1/{project_id}/waf/overviews/abnormal
```

Tabla 4-410 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-411 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.
from	Sí	Long	Hora de inicio (marca de tiempo de 13 dígitos en milisegundos). Este parámetro debe usarse junto con to .
to	Sí	Long	Hora de finalización (marca de tiempo de 13 dígitos en milisegundos). Este parámetro debe usarse junto con from .
top	No	Integer	Los primeros resultados a consultar
code	No	Integer	Código de estado
hosts	No	String	Lista de nombres de dominio a consultar. Se puede obtener llamando a la API ListHost .
instances	No	String	Lista de instancias a consultar (solo para el modo dedicado).

Parámetros de solicitud

Tabla 4-412 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-413 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Tipo de ataque
items	Array of UrlCountItem objects	Detalles de CountItem

Tabla 4-414 UrlCountItem

Parámetro	Tipo	Descripción
key	String	Tipo de ataque
num	Integer	Cantidad
host	String	Nombre de dominio

Código de estado: 400

Tabla 4-415 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-416 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-417 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/abnormal?
enterprise_project_id=0&from=1650470400089&to=1650523520089&top=10&code=404
```

Ejemplo de respuestas

Código de estado: 200

ok

```
{
  "total" : 2,
  "items" : [ {
    "key" : "/",
    "num" : 6,
    "host" : "hkh4.test.418lab.cn"
  }, {
    "key" : "/",
    "num" : 6,
    "host" : "ces_after.test.418lab.cn"
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	ok
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.7 Consulta de características disponibles en un sitio

4.7.1 Consulta de características disponibles en un sitio

Función

Esta API se utiliza para consultar las funciones disponibles en un sitio específico.

URI

GET /v1/{project_id}/waf/config/console

Tabla 4-418 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Parámetros de solicitud

Tabla 4-419 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-420 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
eps	Boolean	Soporte para EPS
tls	Boolean	Versión mínima de TLS soportada. El valor puede ser TLS v1.0, TLS v1.1 o TLS v1.2. TLS v1.0 se utiliza de forma predeterminada.
ipv6	Boolean	Soporte para IPv6
alert	Boolean	Soporte para alarmas
custom	Boolean	Soporte para una protección precisa

Parámetro	Tipo	Descripción
elb_mode	Boolean	Soporte para instancias WAF de equilibrio de carga
event_lts	Boolean	Soporte para LTS para el registro WAF
multi_dns	Boolean	Soporte para resolución multi-DNS
search_ip	Boolean	Soporte para la búsqueda de direcciones IP
cc_enhance	Boolean	Soporte para la mejora de la protección contra ataques CC
cname_switch	Boolean	Soporte para conmutación de registros CNAME
custom_block	Boolean	Soporte para bloques precisos
advanced_ignore	Boolean	Soporte para enmascaramiento de falsa alarma
js_crawler_enable	Boolean	Soporte para antideslizante JavaScript
deep_decode_enable	Boolean	Soporte para análisis detallado
overview_bandwidth	Boolean	Soporte para estadísticas de ancho de banda
proxy_use_oldcname	Boolean	Soporte para la resolución DNS con el antiguo registro CNAME
check_all_headers_enable	Boolean	Soporte para la inspección de todos los encabezados

Código de estado: 400

Tabla 4-421 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-422 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error

Parámetro	Tipo	Descripción
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-423 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/waf/config/console?
enterprise_project_id=0&from=1650470400089&to=1650523520089
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "eps" : true,
  "tls" : true,
  "ipv6" : true,
  "alert" : true,
  "custom" : true,
  "ip_group" : true,
  "event_lts" : true,
  "multi_dns" : true,
  "search_ip" : true,
  "apply_cert" : true,
  "cc_enhance" : true,
  "tms_enable" : true,
  "cname_switch" : true,
  "custom_block" : true,
  "geoip_enable" : true,
  "http2_enable" : true,
  "display_option" : true,
  "advanced_ignore" : true,
  "modulex_enabled" : true,
  "js_crawler_enable" : true,
  "deep_decode_enable" : true,
  "overview_bandwidth" : true,
  "proxy_use_oldcname" : false,
  "load_balance_enable" : true,
  "robot_action_enable" : true,
  "export_domain_enable" : true,
  "policy_sharing_enable" : true,
  "timeout_config_enable" : true,
  "ipv6_protection_enable" : true,
  "check_all_headers_enable" : true,
  "elb_v2" : true,
  "elb_mode" : true,
  "premium_waf_res_tenant" : true
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.8 Consulta de los nombres de dominio de una cuenta

4.8.1 Consulta de la lista de nombres de dominio protegidos

Función

Esta API se utiliza para consultar la lista de nombres de dominio protegidos de una cuenta.

URI

GET /v1/{project_id}/composite-waf/host

Tabla 4-424 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-425 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetro	Obligatorio	Tipo	Descripción
page	No	Integer	Número de página de los datos a devolver durante la consulta de paginación. El valor varía de 0 a 100000 . El valor predeterminado es 1 , que indica que se devuelven los datos de la primera página. Predeterminado: 1
pagesize	No	Integer	Número de resultados en cada página durante la consulta de paginación. El valor varía de 1 a 100 . El valor predeterminado es 10 , lo que indica que cada página contiene 10 resultados. Predeterminado: 10
hostname	No	String	Nombre personalizable para un dominio
policyname	No	String	Política
protect_status	No	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.
waf_type	No	String	Modo WAF del nombre de dominio
is_https	No	Boolean	Si se utiliza HTTPS para el nombre de dominio

Parámetros de solicitud

Tabla 4-426 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-427 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Número total de nombres de dominio protegidos.
cloud_total	Integer	Número de nombres de dominio en modo de cloud
premium_total	Integer	Número de nombres de dominio en modo dedicado
items	Array of CompositeHostResponse objects	Detalles sobre los nombres de dominio

Tabla 4-428 CompositeHostResponse

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio agregado a la nube WAF.
policyid	String	ID de política
access_code	String	Prefijo de CNAME

Parámetro	Tipo	Descripción
protect_status	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.
access_status	Integer	Estado de acceso
proxy	Boolean	Si el proxy está habilitado.
timestamp	Long	Hora en que se agrega un nombre de dominio a WAF.
paid_type	String	Modo de pago basado en paquetes. Actualmente, solo se admite el método de prepago.
flag	HostFlag object	Configuración del nombre de dominio
waf_type	String	Modo de WAF que se utiliza para proteger el nombre de dominio. El valor puede ser cloud o premium . cloud : El WAF cloud se utiliza para proteger el dominio. premium : se utiliza una instancia WAF dedicada para proteger el nombre de dominio.

Tabla 4-429 HostFlag

Parámetro	Tipo	Descripción
pci_dss	String	Verdadero/Falso
pci_3ds	String	Verdadero/Falso
cname	String	antiguo/nuevo
is_dual_az	String	Verdadero/Falso
ipv6	String	Verdadero/Falso

Código de estado: 400

Tabla 4-430 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error

Parámetro	Tipo	Descripción
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-431 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-432 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

POST https://{Endpoint}/v1/{project_id}/composite-waf/host?enterprise_project_id=0

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "items" : [ {
    "id" : "31af669f567246c289771694f2112289",
    "hostid" : "31af669f567246c289771694f2112289",
    "description" : "",
    "type" : 1,
    "proxy" : false,
    "flag" : {
      "pci_3ds" : "false",
      "pci_dss" : "false",
      "ipv6" : "false",
      "cname" : "new",
      "is_dual_az" : "true"
    },
    "region" : "cn-north-4",
    "hostname" : "www.demo.com",
    "access_code" : "1b18879b9d064f8bbcbf8abce7294cac",
    "policyid" : "41cba8aee2e94bcdbf57460874205494",
    "timestamp" : 1650527546454,
    "protect_status" : 0,
  }
]
```

```
"access_status" : 0,  
"exclusive_ip" : false,  
"web_tag" : "",  
"paid_type" : "prePaid",  
"waf_type" : "cloud",  
"bandwidth" : 0,  
"qps" : 0  
} ],  
"total" : 1,  
"cloud_total" : 1,  
"cloud_domain_total" : 1,  
"premium_total" : 0  
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.9 Consulta de un nombre de dominio de una cuenta

4.9.1 Consultar un nombre de dominio por ID

Función

Esta API se utiliza para consultar un nombre de dominio protegido por ID.

URI

GET /v1/{project_id}/composite-waf/host/{host_id}

Tabla 4-433 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Parámetro	Obligatorio	Tipo	Descripción
host_id	Sí	String	ID de nombre de dominio. En el modo de nube, se puede obtener llamando a la API ListHost . En el modo dedicado, se puede obtener llamando a la API ListPremiumHost .

Tabla 4-434 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-435 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8

Parámetros de respuesta

Código de estado: 200

Tabla 4-436 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio agregado a la nube WAF.
policyid	String	ID de política
access_code	String	Prefijo de CNAME

Parámetro	Tipo	Descripción
protect_status	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.
access_status	Integer	Estado de acceso
proxy	Boolean	Si el proxy está habilitado.
timestamp	Long	Hora en que se agrega un nombre de dominio a WAF.
paid_type	String	Modo de pago basado en paquetes. Actualmente, solo se admite el método de prepago.
flag	HostFlag object	Configuración del nombre de dominio
waf_type	String	Modo de WAF que se utiliza para proteger el nombre de dominio. El valor puede ser cloud o premium . cloud : El WAF cloud se utiliza para proteger el dominio. premium : se utiliza una instancia WAF dedicada para proteger el nombre de dominio.

Tabla 4-437 HostFlag

Parámetro	Tipo	Descripción
pci_dss	String	Verdadero/Falso
pci_3ds	String	Verdadero/Falso
cname	String	antiguo/nuevo
is_dual_az	String	Verdadero/Falso
ipv6	String	Verdadero/Falso

Código de estado: 400

Tabla 4-438 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error

Parámetro	Tipo	Descripción
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-439 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-440 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/composite-waf/host/{host_id}?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "31af669f567246c289771694f2112289",
  "hostid" : "31af669f567246c289771694f2112289",
  "description" : "",
  "type" : 1,
  "proxy" : false,
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false",
    "ipv6" : "false",
    "cname" : "new",
    "is_dual_az" : "true"
  },
  "region" : "cn-north-4",
  "hostname" : "www.demo.com",
  "access_code" : "1b18879b9d064f8bbcbf8abce7294cac",
  "policyid" : "41cba8aee2e94bcdbf57460874205494",
  "timestamp" : 1650527546454,
  "protect_status" : 0,
}
```

```
"access_status" : 0,
"exclusive_ip" : false,
"web_tag" : "",
"paid_type" : "prePaid",
"waf_type" : "cloud"
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Error de solicitud.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.10 Gestión de sitios web protegidos en modo dedicado

4.10.1 Adición de un nombre de dominio a una instancia WAF dedicada

Función

Esta API se utiliza para agregar un nombre de dominio a una instancia WAF dedicada.

URI

POST /v1/{project_id}/premium-waf/host

Tabla 4-441 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-442 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-443 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).

Tabla 4-444 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
certificateid	No	String	ID del certificado. Se puede obtener llamando a la API ListCertificates . \n - Este parámetro no es necesario cuando el protocolo cliente es HTTP. \n - Este parámetro es obligatorio cuando el protocolo cliente es HTTPS.
certificatename	No	String	Nombre del certificado. \n - Este parámetro no es necesario cuando el protocolo cliente es HTTP. \n - Este parámetro es obligatorio cuando el protocolo cliente es HTTPS.
hostname	Sí	String	Nombre de dominio protegido o dirección IP (puerto permitido)
proxy	Yes	Boolean	Si se utiliza un proxy para el nombre de dominio

Parámetro	Obligatorio	Tipo	Descripción
policyid	No	String	ID de la política utilizada inicialmente para el nombre de dominio. Se puede obtener llamando a la API ListPolicy .
server	Sí	Array of PremiumWafServer objects	Configuración del servidor

Tabla 4-445 PremiumWafServer

Parámetro	Obligatorio	Tipo	Descripción
front_protocol	Sí	String	Protocolo del cliente Valores de enumeración: ● HTTP ● HTTPS
back_protocol	Sí	String	Protocolo de servidor Valores de enumeración: ● HTTP ● HTTPS
address	Sí	String	Dirección del servidor
port	Sí	Integer	Puerto del servidor
type	Sí	String	La dirección del servidor de origen es una dirección IPv4 o IPv6. Valores de enumeración: ● ipv4 ● ipv6
vpc_id	Sí	String	ID de VPC. Para obtener el ID de VPC, realice los siguientes pasos: ID de VPC. Realice los siguientes pasos para obtener el ID de VPC. \n 1. Inicie sesión en la consola WAF y elija Instance Management > Dedicated Engine > VPC/Subnet . El nombre de la VPC se encuentra en la columna VPC o Subnet . 2. Inicie sesión en la consola de VPC y haga clic en el nombre de VPC. En la página que se muestra, copie el ID en el área VPC Information .

Parámetros de respuesta

Código de estado: 200

Tabla 4-446 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
policyid	String	ID de política
hostname	String	ID de nombre de dominio
domainid	String	ID de inquilino.
projectid	String	ID del proyecto.
protocol	String	Protocolo HTTP

Código de estado: 400

Tabla 4-447 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-448 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-449 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
POST https://{Endpoint}/v1/{project_id}/premium-waf/host?enterprise_project_id=0
{
  "hostname" : "www.demo.com",
  "server" : [ {
    "front_protocol" : "HTTP",
    "back_protocol" : "HTTP",
    "vpc_id" : "cf6dbace-b36a-4d51-ae04-52a3319ae247",
    "type" : "ipv4",
    "address" : "x.x.x.x",
    "port" : 80
  } ],
  "proxy" : false,
  "description" : ""
}
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "51a5649e52d341a9bb802044950969dc",
  "hostname" : "www.demo.com",
  "protocol" : "HTTP",
  "server" : [ {
    "address" : "x.x.x.x",
    "port" : 80,
    "type" : "ipv4",
    "weight" : 1,
    "front_protocol" : "HTTP",
    "back_protocol" : "HTTP",
    "vpc_id" : "cf6dbace-b36a-4d51-ae04-52a3319ae247"
  } ],
  "proxy" : false,
  "locked" : 0,
  "timestamp" : 1650596007113,
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false"
  },
  "description" : "",
  "policyid" : "1607df035bc847b582ce9c838c083b88",
  "domainid" : "d4ecb00b031941ce9171b7bc3386883f",
  "enterprise_project_id" : "0",
  "protect_status" : 1,
  "access_status" : 0,
  "web_tag" : "",
  "access_progress" : [ ]
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Solicitud no válida.
401	Permisos de token insuficientes.

Código de estado	Descripción
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.10.2 Consulta de nombres de dominio protegidos por motores WAF dedicados

Función

Esta API se utiliza para consultar la lista de nombres de dominio conectados a instancias de WAF dedicadas.

URI

GET /v1/{project_id}/premium-waf/host

Tabla 4-450 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto

Tabla 4-451 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.
page	No	String	Número de página de los datos a devolver durante la consulta de paginación. El valor varía de 0 a 100000 . El valor predeterminado es 1 , que indica que se devuelven los datos de la primera página. Predeterminado: 1

Parámetro	Obligatorio	Tipo	Descripción
pagesize	No	String	Número de resultados en cada página durante la consulta de paginación. El valor varía de 1 a 100 . El valor predeterminado es 10 , lo que indica que cada página contiene 10 resultados. Predeterminado: 10
hostname	No	String	Nombre de dominio
policyname	No	String	Nombre de la política.
protect_status	No	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.

Parámetros de solicitud

Tabla 4-452 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).

Parámetros de respuesta

Código de estado: **200**

Tabla 4-453 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
total	Integer	Número total de nombres de dominio protegidos
items	Array of SimplePremiumWafHost objects	Detalles sobre el nombre de dominio protegido

Tabla 4-454 SimplePremiumWafHost

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio
policyid	String	ID de política
protect_status	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.
access_status	Integer	Estado de acceso
flag	Map<String,String>	Identificador especial
mode	String	Identificador del motor WAF dedicado en modo WAF especial, como ELB.
pool_ids	Array of strings	Clúster de motor dedicado al que pertenece el nombre de dominio

Código de estado: 400

Tabla 4-455 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-456 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-457 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/premium-waf/host?enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "ee896796e1a84f3f85865ae0853d8974",
    "hostname" : "www.demo.com",
    "extend" : { },
    "region" : "cn-north-7",
    "flag" : {
      "pci_3ds" : "false",
      "pci_dss" : "false"
    },
    "description" : "",
    "policyid" : "df15d0eb84194950a8fdc615b6c012dc",
    "protect_status" : 1,
    "access_status" : 0,
    "hostid" : "ee896796e1a84f3f85865ae0853d8974"
  } ]
}
```

Códigos de estado

Código de estado	Descripción
200	OK

Código de estado	Descripción
400	Solicitud no válida.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.10.3 Modificación de un nombre de dominio protegido por una instancia WAF dedicada

Función

Esta API se utiliza para modificar la configuración de un nombre de dominio conectado a una instancia WAF dedicada.

URI

PUT /v1/{project_id}/premium-waf/host/{host_id}

Tabla 4-458 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
host_id	Sí	String	ID del nombre de dominio protegido por el motor WAF dedicado

Tabla 4-459 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API <code>ListEnterpriseProject</code> de EPS.

Parámetros de solicitud

Tabla 4-460 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
Content-Type	Sí	String	Tipo de contenido. Predeterminado: application/json;charset=utf8
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).

Tabla 4-461 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
proxy	No	Boolean	Si se utiliza un proxy para el nombre de dominio
certificateid	No	String	ID de certificado HTTPS. Se puede obtener llamando a la API ListCertificates .
certificatename	No	String	Nombre del certificado HTTPS. Se puede obtener llamando a la API ListCertificates .
tls	No	String	Versión de TLS mínima Valores de enumeración: <ul style="list-style-type: none"> ● TLS v1.0 ● TLS v1.1 ● TLS v1.2 ● TLS v1.3

Parámetro	Obligatorio	Tipo	Descripción
cipher	No	String	<p>Conjunto de cifrado. El valor puede ser cipher_1, cipher_2, cipher_3, cipher_4, or cipher_default: \n cipher_1: Los algoritmos criptográficos son ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH. \n cipher_2: Los algoritmos criptográficos son ECDH+AESGCM:EDH+AESGCM. \n cipher_3: Los algoritmos criptográficos son ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH. \n cipher_4: Los algoritmos criptográficos son ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH. \n cipher_default: Los algoritmos criptográficos son ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM.</p> <p>Valores de enumeración:</p> <ul style="list-style-type: none"> ● cipher_1 ● cipher_2 ● cipher_3 ● cipher_4 ● cipher_default

Parámetros de respuesta

Código de estado: 200

Tabla 4-462 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
policyid	String	ID de la política utilizada inicialmente para el nombre de dominio. Se puede obtener llamando a la API ListPolicy .
hostname	String	Nombre de dominio conectado a una instancia WAF en la nube
domainid	String	ID de dominio de usuario
project_id	String	ID del proyecto
access_code	String	Prefijo de CNAME
protocol	String	Protocolo HTTP
server	Array of PremiumWafServer objects	Detalles del servidor de origen
certificateid	String	ID del certificado. Se puede obtener llamando a la API ListCertificates . \n - Este parámetro no es necesario cuando el protocolo cliente es HTTP. \n - Este parámetro es obligatorio cuando el protocolo cliente es HTTPS.
certificatename	String	Nombre del certificado. \n - Este parámetro no es necesario cuando el protocolo cliente es HTTP. \n - Este parámetro es obligatorio cuando el protocolo cliente es HTTPS.
tls	String	Versión mínima de TLS soportada. El valor puede ser TLS v1.0, TLS v1.1 o TLS v1.2. TLS v1.0 se utiliza de forma predeterminada. Valores de enumeración: <ul style="list-style-type: none"> ● TLS v1.0 ● TLS v1.1 ● TLS v1.2 ● TLS v1.3

Parámetro	Tipo	Descripción
cipher	String	<p>Conjunto de cifrado. El valor puede ser cipher_1, cipher_2, cipher_3, cipher_4, or cipher_default: \n cipher_1: Los algoritmos criptográficos son ECDHE-ECDHE-RSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH. \n cipher_2: Los algoritmos criptográficos son ECDH+AESGCM:EDH+AESGCM. \n cipher_3: The cryptographic algorithms are ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH. \n cipher_4: Los algoritmos criptográficos son ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH. \n cipher_default: Los algoritmos criptográficos son ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM.</p> <p>Valores de enumeración:</p> <ul style="list-style-type: none"> ● cipher_1 ● cipher_2 ● cipher_3 ● cipher_4 ● cipher_default
proxy	Boolean	Si el proxy está habilitado
locked	Integer	Estado de bloqueo Predeterminado: 0
protect_status	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.
access_status	Integer	Estado de acceso
timestamp	Long	Hora en que se conectó el nombre de dominio a WAF
block_page	BlockPage object	Página de configuración de alarma

Parámetro	Tipo	Descripción
extend	Map<String,String>	atributo extendido
traffic_mark	TrafficMark object	Identificador de tráfico (utilizado para reglas de origen de ataque conocidas)
flag	Map<String,String>	Etiqueta de nombre de dominio especial
mode	String	Nodo de nombre de dominio especial en modo dedicado. Este parámetro solo se requiere para modos WAF especiales, como ELB.
pool_ids	Array of strings	ID de grupo asociado con el nombre de dominio. Este parámetro solo se requiere en modos especiales, como ELB.

Tabla 4-463 PremiumWafServer

Parámetro	Tipo	Descripción
front_protocol	String	Protocolo del cliente Valores de enumeración: <ul style="list-style-type: none"> ● HTTP ● HTTPS
back_protocol	String	Protocolo de servidor Valores de enumeración: <ul style="list-style-type: none"> ● HTTP ● HTTPS
address	String	Dirección del servidor
port	Integer	Puerto del servidor
type	String	La dirección del servidor de origen es una dirección IPv4 o IPv6. Valores de enumeración: <ul style="list-style-type: none"> ● ipv4 ● ipv6

Parámetro	Tipo	Descripción
vpc_id	String	ID de VPC. Para obtener el ID de VPC, realice los siguientes pasos: ID de VPC. Realice los siguientes pasos para obtener el ID de VPC. \n 1. Inicie sesión en la consola WAF y elija Instance Management > Dedicated Engine > VPC/Subnet . El nombre de la VPC se encuentra en la columna VPC o Subnet . 2. Inicie sesión en la consola de VPC y haga clic en el nombre de VPC. En la página que se muestra, copie el ID en el área VPC Information .

Tabla 4-464 BlockPage

Parámetro	Tipo	Descripción
template	String	Nombre de la plantilla
custom_page	CustomPage object	Página de alarma personalizada
redirect_url	String	URL de redireccionamiento

Tabla 4-465 CustomPage

Parámetro	Tipo	Descripción
status_code	String	Códigos de estado
content_type	String	Tipo de contenido de la página de alarma
content	String	Contenido de la página

Tabla 4-466 TrafficMark

Parámetro	Tipo	Descripción
sip	Array of strings	Dirección IP en la regla de origen de ataque conocida
cookie	String	cookie
params	String	Parámetros

Código de estado: 400

Tabla 4-467 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-468 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-469 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
{
  "proxy" : false
}
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "27995fb98a2d4928a1e453e65ee8117a",
  "hostname" : "www.demo.com",
  "protocol" : "HTTP",
  "server" : [ {
    "address" : "192.168.0.209",
    "port" : 80,
    "type" : "ipv4",
    "weight" : 1,
    "front_protocol" : "HTTP",
    "back_protocol" : "HTTP",
    "vpc_id" : "cf6dbace-b36a-4d51-ae04-52a8459ae247"
  } ],
  "proxy" : false,
```

```

"locked" : 0,
"timestamp" : 1650590814885,
"flag" : {
  "pci_3ds" : "false",
  "pci_dss" : "false"
},
"description" : "",
"policyid" : "9555cda636ef4ca294dfe4b14bc94c47",
"domainid" : "d4ecb00b031941ce9171b7bc3386883f",
"projectid" : "05e33ecd328025dd2f7fc00696201fb4",
"enterprise_project_id" : "0",
"protect_status" : 1,
"access_status" : 0
}

```

Códigos de estado

Código de estado	Descripción
200	OK
400	Solicitud no válida.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.10.4 Configuración de consultas de nombres de dominio protegidos con instancias WAF dedicadas

Función

Esta API se utiliza para consultar la configuración de nombres de dominio protegidos con instancias WAF dedicadas.

URI

GET /v1/{project_id}/premium-waf/host/{host_id}

Tabla 4-470 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
host_id	Sí	String	ID del nombre de dominio protegido por el motor WAF dedicado

Tabla 4-471 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-472 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).

Parámetros de respuesta

Código de estado: 200

Tabla 4-473 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
policyid	String	ID de la política utilizada inicialmente para el nombre de dominio. Se puede obtener llamando a la API ListPolicy .
hostname	String	Nombre de dominio conectado a una instancia WAF en la nube
domainid	String	ID de dominio de usuario
project_id	String	ID del proyecto
access_code	String	Prefijo de CNAME
protocol	String	Protocolo HTTP

Parámetro	Tipo	Descripción
server	Array of PremiumWafServer objects	Detalles del servidor de origen
certificateid	String	ID del certificado. Se puede obtener llamando a la API ListCertificates . \n - Este parámetro no es necesario cuando el protocolo cliente es HTTP. \n - Este parámetro es obligatorio cuando el protocolo cliente es HTTPS.
certificatename	String	Nombre del certificado. \n - Este parámetro no es necesario cuando el protocolo cliente es HTTP. \n - Este parámetro es obligatorio cuando el protocolo cliente es HTTPS.
tls	String	Versión mínima de TLS soportada. El valor puede ser TLS v1.0, TLS v1.1 o TLS v1.2. TLS v1.0 se utiliza de forma predeterminada. Valores de enumeración: <ul style="list-style-type: none"> ● TLS v1.0 ● TLS v1.1 ● TLS v1.2 ● TLS v1.3

Parámetro	Tipo	Descripción
cipher	String	<p>Conjunto de cifrado. El valor puede ser cipher_1, cipher_2, cipher_3, cipher_4, or cipher_default: \n cipher_1: Los algoritmos criptográficos son ECDHE-ECDHE-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH. \n cipher_2: Los algoritmos criptográficos son ECDH+AESGCM:EDH+AESGCM. \n cipher_3: The cryptographic algorithms are ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH. \n cipher_4: Los algoritmos criptográficos son ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH. \n cipher_default: Los algoritmos criptográficos son ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM.</p> <p>Valores de enumeración:</p> <ul style="list-style-type: none"> ● cipher_1 ● cipher_2 ● cipher_3 ● cipher_4 ● cipher_default
proxy	Boolean	Si el proxy está habilitado
locked	Integer	Estado de bloqueo Predeterminado: 0
protect_status	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.
access_status	Integer	Estado de acceso
timestamp	Long	Hora en que se conectó el nombre de dominio a WAF
block_page	BlockPage object	Página de configuración de alarma

Parámetro	Tipo	Descripción
extend	Map<String,String>	atributo extendido
traffic_mark	TrafficMark object	Identificador de tráfico (utilizado para reglas de origen de ataque conocidas)
flag	Map<String,String>	Etiqueta de nombre de dominio especial
mode	String	Nodo de nombre de dominio especial en modo dedicado. Este parámetro solo se requiere para modos WAF especiales, como ELB.
pool_ids	Array of strings	ID de grupo asociado con el nombre de dominio. Este parámetro solo se requiere en modos especiales, como ELB.

Tabla 4-474 PremiumWafServer

Parámetro	Tipo	Descripción
front_protocol	String	Protocolo del cliente Valores de enumeración: <ul style="list-style-type: none"> ● HTTP ● HTTPS
back_protocol	String	Protocolo de servidor Valores de enumeración: <ul style="list-style-type: none"> ● HTTP ● HTTPS
address	String	Dirección del servidor
port	Integer	Puerto del servidor
type	String	La dirección del servidor de origen es una dirección IPv4 o IPv6. Valores de enumeración: <ul style="list-style-type: none"> ● ipv4 ● ipv6

Parámetro	Tipo	Descripción
vpc_id	String	ID de VPC. Para obtener el ID de VPC, realice los siguientes pasos: ID de VPC. Realice los siguientes pasos para obtener el ID de VPC. \n 1. Inicie sesión en la consola WAF y elija Instance Management > Dedicated Engine > VPC/Subnet . El nombre de la VPC se encuentra en la columna VPC o Subnet . 2. Inicie sesión en la consola de VPC y haga clic en el nombre de VPC. En la página que se muestra, copie el ID en el área VPC Information .

Tabla 4-475 BlockPage

Parámetro	Tipo	Descripción
template	String	Nombre de la plantilla
custom_page	CustomPage object	Página de alarma personalizada
redirect_url	String	URL de redireccionamiento

Tabla 4-476 CustomPage

Parámetro	Tipo	Descripción
status_code	String	Códigos de estado
content_type	String	Tipo de contenido de la página de alarma
content	String	Contenido de la página

Tabla 4-477 TrafficMark

Parámetro	Tipo	Descripción
sip	Array of strings	Dirección IP en la regla de origen de ataque conocida
cookie	String	cookie
params	String	Parámetros

Código de estado: 400

Tabla 4-478 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-479 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-480 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
GET https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "ee896796e1a84f3f85865ae0853d8974",
  "hostname" : "www.demo.com",
  "protocol" : "HTTPS",
  "server" : [ {
    "address" : "1.2.3.4",
    "port" : 443,
    "type" : "ipv4",
    "weight" : 1,
    "front_protocol" : "HTTPS",
    "back_protocol" : "HTTPS",
    "vpc_id" : "ebfc553a-386d-4746-b0c2-18ff3f0e903d"
  } ],
  "proxy" : false,
  "locked" : 0,
```

```

"timestamp" : 1650593801380,
"tls" : "TLS v1.0",
"cipher" : "cipher_1",
"flag" : {
  "pci_3ds" : "false",
  "pci_dss" : "false"
},
"description" : "",
"policyid" : "df15d0eb84194950a8fdc615b6c012dc",
"domainid" : "0ee78615ca08419f81f539d97c9ee353",
"projectid" : "550500b49078408682d0d4f7d923f3e1",
"protect_status" : 1,
"access_status" : 0,
"certificateid" : "360f992501a64de0a65c50a64d1ca7b3",
"certificatename" : "certificatename75315"
}

```

Códigos de estado

Código de estado	Descripción
200	OK
400	Solicitud no válida.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.10.5 Eliminación de un nombre de dominio de una instancia WAF dedicada

Función

Esta API se utiliza para eliminar un nombre de dominio protegido con una instancia WAF dedicada.

URI

DELETE /v1/{project_id}/premium-waf/host/{host_id}

Tabla 4-481 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
host_id	Sí	String	ID del nombre de dominio protegido por el motor WAF dedicado

Tabla 4-482 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.
keepPolicy	No	Boolean	Si se debe conservar la regla Predeterminado: 1

Parámetros de solicitud

Tabla 4-483 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json;charset=utf8
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).

Parámetros de respuesta

Código de estado: 200

Tabla 4-484 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
id	String	ID de nombre de dominio
hostname	String	Nombre de dominio
policyid	String	ID de política
region	String	ID de región.

Parámetro	Tipo	Descripción
protect_status	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.
access_status	Integer	Estado de acceso
flag	Map<String,String>	Identificador especial
mode	String	Identificador del motor WAF dedicado en modo WAF especial, como ELB.
pool_ids	Array of strings	Clúster de motor dedicado al que pertenece el nombre de dominio

Código de estado: 400

Tabla 4-485 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 401

Tabla 4-486 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-487 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
DELETE https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}?
enterprise_project_id=0
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "id" : "ee896796e1a84f3f85865ae0853d8974",
  "hostname" : "www.demo.com",
  "region" : "cn-north-7",
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false"
  },
  "description" : "",
  "policyid" : "df15d0eb84194950a8fdc615b6c012dc",
  "protect_status" : 1,
  "access_status" : 0,
  "hostid" : "ee896796e1a84f3f85865ae0853d8974"
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Solicitud no válida.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

4.10.6 Modificación del estado de protección de un nombre de dominio en modo dedicado

Función

Esta API se utiliza para modificar el estado de protección de un nombre de dominio protegido con una instancia WAF dedicada.

URI

PUT /v1/{project_id}/premium-waf/host/{host_id}/protect-status

Tabla 4-488 Parámetros de ruta

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto
host_id	Sí	String	ID del nombre de dominio protegido por el motor WAF dedicado

Tabla 4-489 Parámetros de consulta

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto de empresa. Se puede obtener mediante el llamado API ListEnterpriseProject de EPS.

Parámetros de solicitud

Tabla 4-490 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
Content-Type	Sí	String	Tipo de contenido Predeterminado: application/json; charset=utf8
X-Auth-Token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de X-Subject-Token en el encabezado de respuesta).

Tabla 4-491 Parámetros del cuerpo de solicitud

Parámetro	Obligatorio	Tipo	Descripción
protect_status	Sí	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.

Parámetros de respuesta

Código de estado: 200

Tabla 4-492 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
protect_status	Integer	Estado de protección del nombre de dominio. \n - -1 : Se omite la protección WAF. Las solicitudes del nombre de dominio se envían directamente al servidor backend y no pasan a través de WAF. \n - 0 : La protección WAF está suspendida. WAF solo reenvía solicitudes del nombre de dominio y no detecta ataques. \n - 1 : La protección WAF está habilitada. WAF detecta ataques basados en la política configurada.

Código de estado: 400

Tabla 4-493 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estad: 401

Tabla 4-494 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Código de estado: 500

Tabla 4-495 Parámetros del cuerpo de respuesta

Parámetro	Tipo	Descripción
error_code	String	Código de error
error_msg	String	Mensaje de código de error

Solicitudes de ejemplo

```
PUT https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}/protect-status?
enterprise_project_id=0
```

```
{
  "protect_status" : 1
}
```

Ejemplo de respuestas

Código de estado: 200

OK

```
{
  "protect_status" : 1
}
```

Códigos de estado

Código de estado	Descripción
200	OK
400	Solicitud no válida.
401	Permisos de token insuficientes.
500	Error de servidor interno.

Códigos de error

Consulte [Códigos de error](#).

A Apéndice

A.1 Código de estado

- Normal

Valores devueltos	Descripción
200	La solicitud se procesa correctamente.

- Anormal

Código de estado	Estado	Descripción
400	Bad Request	El servidor no puede procesar la solicitud.
401	Unauthorized	La página solicitada requiere un nombre de usuario y una contraseña.
403	Forbidden	El acceso a la página solicitada no se encuentra disponible.
404	Not Found	El servidor no encuentra la página solicitada.
405	Method Not Allowed	El método especificado en la solicitud no está permitido.
406	Not Acceptable	La respuesta generada por el servidor no es aceptable para el cliente.
407	Proxy Authentication Required	Se requiere autenticación de proxy antes de procesar la solicitud.
408	Request Timeout	Se produce un error de tiempo de espera porque la solicitud no se procesa dentro del período de espera especificado del servidor.

Código de estado	Estado	Descripción
409	Conflict	La solicitud no se puede procesar debido a un conflicto.
500	Internal Server Error	La solicitud no se procesa debido a un error del servidor.
501	Not Implemented	La solicitud no se procesa porque el servidor no admite la función solicitada.
502	Bad Gateway	La solicitud no se procesa y el servidor recibe una respuesta no válida del servidor ascendente.
503	Service Unavailable	La solicitud no se procesa debido a una anomalía temporal del sistema.
504	Gateway Timeout	Se produce un error de tiempo de espera de la puerta de enlace.

A.2 Códigos de error

Si se devuelve un código de error que comienza con APIGW después de llamar a una API, corrija el error haciendo referencia a las instrucciones proporcionadas en [Códigos de error de puerta de enlace API](#).

Código de estado	Códigos de error	Mensaje de error	Descripción	Solución
400	WAF.00011001	bad.request	Error en la solicitud	Comprobar param
400	WAF.00011002	url.param.illegal	El formato de URL es incorrecto	Comprobar formato de URL
400	WAF.00011003	request.body.illegal	Error de formato del cuerpo de la solicitud: falta parámetro y valor ilegal en el cuerpo	Comprobar el cuerpo de la solicitud
400	WAF.00011004	id.illegal	ID ilegal	Comprobar ID
400	WAF.00011005	name.illegal	Nombre ilegal	Comprobar nombre

Código de estado	Códigos de error	Mensaje de error	Descripción	Solución
400	WAF.00011006	host.illegal	Nombre de dominio no autorizado	Comprobar nombre de dominio
400	WAF.00011007	port.illegal	Puerto ilegal	Comprobar puerto
400	WAF.00011007	ip.illegal	IP ilegal	Comprobar IP
400	WAF.00011008	protect.status.illegal	Estado de protección ilegal	Comprobar si el estado de protección está en el rango del valor de enumeración
400	WAF.00011009	access.status.illegal	Estado de acceso ilegal	Comprobar si el estado de acceso está en el rango de valor de enumeración
400	WAF.00011010	offsetOrLimit.illegal	Desplazamiento ilegal o número límite	Compruebe si la línea inicial o el número límite está dentro del rango
400	WAF.00011011	pageOrPageSize.illegal	Número de página ilegal o número de entradas por página	Comprobar si el número de página o el número de elementos por página están en el rango
400	WAF.00011012	standard.violated	Parámetro no válido	Comprobar los parámetros
400	WAF.00011013	description.illegal	Formato de descripción ilegal	Comprobar el formato de descripción
400	WAF.00011014	request.header.illegal	Error de formato de encabezado de solicitud: parámetro faltante y valor ilegal en el encabezado	Comprobar los parámetros requeridos del encabezado
400	WAF.00011014	website.not.register	El sitio web no ha sido puesto en registro	Sitio web de presentación

Código de estado	Códigos de error	Mensaje de error	Descripción	Solución
400	WAF.00012001	invalid.token	Token ilegal	Comprobar si el token es correcto
400	WAF.00012002	invalid.project	Incoherencia entre project_id y token	Comprobar Coherencia de project_id y token
400	WAF.00012003	permission.denied	Sin permiso	Asignar los permisos necesarios de WAF a la cuenta
400	WAF.00012004	account.frozen	Congelación de cuentas	Descongelación de cuenta
400	WAF.00012005	not.subscribe	Anulación de suscripción	Suscribase al servicio WAF primero
400	WAF.00012006	pdp.permission.denied	Sin permiso	Comprobar la autoridad PDP de la cuenta
400	WAF.00012007	jwt.authentication.disabled	Certificación JWT desactivada	Certificación JWT abierta
400	WAF.00012008	jwt.authentication.invalid.token	Token JWT ilegal	Comprobar si la cuenta tiene permiso JWT
400	WAF.00012009	jwt.authentication.failed	Error de autenticación JWT	Dar la autorización de la cuenta primero
400	WAF.00012010	eps.all.not.support	eps.all.not.support	Abrir el permiso de escritura del proyecto de empresa
400	WAF.00013001	insufficient.quota	Cuota de funciones insuficiente	Paquete de actualización de cuota de función de compra
400	WAF.00013002	feature.not.support	Función no soportada	nada
400	WAF.00013003	port.not.support	Puerto no soportado	Conversión de puertos a través de ELB
400	WAF.00013004	protocol.not.support	No se admite el protocolo	A través del protocolo de conversión ELB

Código de estado	Códigos de error	Mensaje de error	Descripción	Solución
400	WAF.00013005	wildcard.domain.not.support	No se admite el nombre de dominio de Pan	Usar nombres de dominio específicos
400	WAF.00013006	ipv6.not.support	No se admite IPv6	La versión actual no admite IPv6
400	WAF.00013007	insufficient.tenant.quota	cuota de inquilino insuficiente	Paquete de actualización de cuota de compra
400	WAF.00014001	resource.not.found	No se encuentra el recurso	El recurso se ha eliminado o no existe
400	WAF.00014002	resource.already.exists	El recurso ya existe	El recurso ya existe
400	WAF.00014003	open.protect.failed	Error al abrir la protección	Comprobar el estado de protección del nombre de dominio
400	WAF.00014004	access.failed	Error al acceder a WAF	Modificar la resolución DNS
400	WAF.00014005	bypass.failed	Error de bypasswaf	Comprobar el estado de protección e inténtelo de nuevo
400	WAF.00014006	proxy.config.error	Error de configuración del agente	Reconfigurar el agente correctamente e intentar de nuevo
400	WAF.00014007	host.conflict	Conflicto de nombres de dominio	Comprobar que el nombre de dominio ya existe en la configuración del sitio web
400	WAF.00014008	cert.inconsistent	El mismo nombre de dominio, pero el certificado es inconsistente	Utilizar el mismo certificado
400	WAF.00014009	api.not.found	La interfaz no existe	Comprobar URL de interfaz
400	WAF.00014010	port.protocol.mismatch	No concordancia de puertos y protocolos	Seleccione el protocolo y el puerto correspondientes

Código de estado	Códigos de error	Mensaje de error	Descripción	Solución
400	WAF.00014011	host.blacklist	Está prohibido agregar el sitio web de protección, y el nombre de dominio está en la lista negra	
400	WAF.00014012	insufficient.tenant.quota	Cuota de inquilino insuficiente	Paquete de actualización de cuota de compra
400	WAF.00014013	exclusive.ip.config.error	Error de configuración IP exclusivo	Comprobar la configuración IP exclusiva
400	WAF.00014014	exclusive.ip.config.error	exclusive.ip.config.error	Comprobar la configuración IP exclusiva
500	WAF.00010001	internal.error	Error interno	Contactar con el soporte técnico
500	WAF.00010002	system.busy	Error interno	Contactar con el soporte técnico
500	WAF.00010003	cname.failed	Error al crear o modificar CNAME	Contactar con el soporte técnico
500	WAF.00010004	cname.failed	Error al obtener el enlace de descarga del archivo OBS	Contactar con el soporte técnico

A.3 Obtención de un ID de proyecto

Obtención de un ID de proyecto llamando a una API

Puede obtener el ID del proyecto llamando a la API utilizada para [consultar información del proyecto en función de los criterios especificados](#).

La API utilizada para obtener un ID de proyecto es GET `https://{Endpoint}/v3/projects`. **{Endpoint}** es el endpoint de IAM y se puede obtener de [Regiones and endpoint](#). Para obtener más información sobre la autenticación de API, consulte [Autenticación](#).

En el siguiente ejemplo, **id** indica el ID del proyecto.

```
{
  "projects": [
    {
```

```

    "domain_id": "65382450e8f64ac0870cd180d14e684b",
    "is_domain": false,
    "parent_id": "65382450e8f64ac0870cd180d14e684b",
    "name": "xxxxxxx",
    "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"
}
}

```

Obtención de un ID de proyecto desde la consola

Se requiere un ID de proyecto para algunas URL cuando se llama a una API. Para obtener un ID de proyecto, realice las siguientes operaciones:

1. Inicie sesión en la consola de gestión.
2. Haga clic en el nombre de usuario y elija **Basic Information** en la lista desplegable.
3. En la página **Account Info**, haga clic en **Manage** junto a **Security Credentials**.
En la página **My Credentials**, vea los ID de proyecto en la lista de proyectos.

Figura A-1 Consulta de IDs de proyecto

