

# Web Application Firewall

## Referência de API

Edição 01  
Data 01-11-2022



**Copyright © Huawei Technologies Co., Ltd. 2022. Todos os direitos reservados.**

Nenhuma parte deste documento pode ser reproduzida ou transmitida em qualquer forma ou por qualquer meio sem consentimento prévio por escrito da Huawei Technologies Co., Ltd.

### **Marcas registadas e permissões**



HUAWEI e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd. Todos as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

### **Aviso**

Os produtos, serviços e funcionalidades adquiridos são estipulados pelo contrato feito entre a Huawei e o cliente. Todos ou parte dos produtos, serviços e funcionalidades descritos neste documento pode não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÁ" sem garantias, ou representações de qualquer tipo, seja expressa ou implícita.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. Foram feitos todos os esforços na preparação deste documento para assegurar a exatidão do conteúdo, mas todas as declarações, informações e recomendações contidas neste documento não constituem uma garantia de qualquer tipo, expressa ou implícita.

## **Huawei Technologies Co., Ltd.**

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

Site: <https://www.huawei.com>

Email: [support@huawei.com](mailto:support@huawei.com)

---

# Índice

---

<b>1 Antes de começar.....</b>	<b>1</b>
1.1 Visão geral.....	1
1.2 Chamada de API.....	1
1.3 Conceitos.....	1
<b>2 Visão geral da API.....</b>	<b>3</b>
<b>3 Chamada de API.....</b>	<b>4</b>
3.1 Criação de uma solicitação de API.....	4
3.2 Autenticação.....	7
3.3 Resposta.....	8
<b>4 API.....</b>	<b>10</b>
4.1 Gerenciamento de sites protegidos no modo nuvem.....	10
4.1.1 Essa API é usada para consultar a lista de nomes de domínio protegidos no modo nuvem.....	10
4.1.2 Adição de um nome de domínio ao Cloud WAF.....	16
4.1.3 Consulta de detalhes sobre um nome de domínio por ID de nome de domínio no modo nuvem.....	27
4.1.4 Atualização de configurações de nomes de domínio protegidos com o Cloud WAF.....	38
4.1.5 Exclusão de um nome de domínio do Cloud WAF.....	57
4.1.6 Alteração de status de proteção de um nome de domínio.....	62
4.1.7 Obtenção de informações de roteamento de nome de domínio (no modo nuvem).....	65
4.2 Gerenciamento de sites protegidos por mecanismos dedicados do WAF.....	69
4.2.1 Consulta de nomes de domínio protegidos por mecanismos WAF dedicados.....	69
4.2.2 Adição de um nome de domínio a uma instância dedicada do WAF.....	75
4.2.3 Modificação de um nome de domínio protegido por uma instância WAF dedicada.....	86
4.2.4 Consulta de configurações de nome de domínio no modo dedicado.....	102
4.2.5 Exclusão de um nome de domínio de uma instância dedicada do WAF.....	111
4.2.6 Modificação de status de proteção de um nome de domínio no modo dedicado.....	116
4.3 Gerenciamento de políticas.....	120
4.3.1 Consulta de lista de políticas de proteção.....	120
4.3.2 Criação de uma política de proteção.....	128
4.3.3 Consulta de uma política por ID.....	136
4.3.4 Atualização de uma política de proteção.....	144
4.3.5 Exclusão de uma política de proteção.....	156
4.3.6 Atualização da política de proteção de nomes de domínio.....	164

4.4 Gerenciamento de regras.....	172
4.4.1 Alteração de status de uma regra.....	172
4.4.2 Consulta de regras da lista branca de proteção global (Anteriormente mascaramento de alarmes falsos).....	175
4.4.3 Criação de uma regra de lista branca de proteção global (Anteriormente mascaramento de alarme falso).....	181
4.4.4 Exclusão de uma regra de lista branca de proteção global (Anteriormente mascaramento de alarme falso).....	189
4.4.5 Consulta de lista de regras da lista negra e da lista branca.....	194
4.4.6 Criação de uma regra de lista negra/lista branca.....	197
4.4.7 Atualização de uma regra de proteção de lista negra ou lista branca.....	202
4.4.8 Exclusão de uma regra de lista negra ou de lista branca.....	206
4.4.9 Consulta de uma regra de mascaramento de dados.....	209
4.4.10 Criação de uma regra de mascaramento de dados.....	213
4.4.11 Atualização de uma regra de mascaramento de dados.....	218
4.4.12 Exclusão de uma regra de mascaramento de dados.....	223
4.4.13 Consulta de lista de regras de controle de acesso de geolocalização.....	226
4.4.14 Atualização de uma regra de controle de acesso de geolocalização.....	230
4.4.15 Atualização de uma regra de controle de acesso de geolocalização.....	235
4.4.16 Exclusão de uma regra de controle de acesso de geolocalização.....	240
4.4.17 Consulta de lista de regras de proteção contra intrusão na Web.....	244
4.4.18 Criação de uma regra de proteção contra violação da Web.....	247
4.4.19 Exclusão de uma regra de proteção contra violação da Web.....	251
4.4.20 Consulta de lista de tabelas de referência.....	254
4.4.21 Criação de uma tabela de referência.....	258
4.4.22 Modificação de uma tabela de referência.....	261
4.4.23 Exclusão de uma tabela de referência.....	265
4.5 Gerenciamento de certificado.....	268
4.5.1 Consulta de lista de certificados.....	268
4.5.2 Carregamento de um certificado.....	272
4.5.3 Consulta de um certificado.....	277
4.5.4 Modificação de um certificado.....	281
4.5.5 Exclusão de um certificado.....	284
4.5.6 Aplicação de um certificado a um nome de domínio.....	287
4.6 Gerenciamento de eventos.....	291
4.6.1 Consulta de lista de eventos de ataque.....	291
4.6.2 Essa API é usada para consultar detalhes sobre um evento de um ID especificado.....	298
4.7 Painel de controle.....	301
4.7.1 Consulta de estatísticas de solicitações e ataques.....	302
4.7.2 Consulta de estatísticas do QPS.....	306
4.7.3 Consulta de estatísticas de uso da largura de banda.....	310
4.7.4 Consulta de estatísticas das principais exceções.....	314
4.7.5 Consulta de principais estatísticas de segurança por categoria.....	318
4.7.6 Consulta de solicitações de sites.....	324
4.8 Consulta de nome de domínio de um inquilino.....	328

---

4.8.1 Consulta de nomes de domínio protegidos com todas as instâncias do WAF.....	329
4.8.2 Consulta de um nome de domínio por ID.....	336
4.9 Consulta de recursos disponíveis em um site.....	342
4.9.1 Recursos de consulta disponíveis em um site.....	342
<b>A Apêndice.....</b>	<b>348</b>
A.1 Código de status.....	348
A.2 Códigos de erro.....	349
A.3 Obtenção de ID de projeto.....	356

# 1 Antes de começar

---

## 1.1 Visão geral

Web Application Firewall (WAF) mantém os serviços web estáveis e seguros. Ele examina todas as solicitações HTTP e HTTPS para detectar e bloquear os seguintes ataques: Injeção de linguagem de consulta estruturada (SQL), cross-site scripting (XSS), web shells, injeções de comando e código, inclusão de arquivos, acesso a arquivos sensíveis, explorações de vulnerabilidade de terceiros, ataques Challenge Collapsar (CC), rastreadores maliciosos, e falsificação de solicitação entre sites (CSRF).

Este documento descreve como usar interfaces de programação de aplicativos (as API) para executar operações no WAF, como consultas e atualizações.

Antes de começar, certifique-se de que você está familiarizado com o WAF. Para obter detalhes, consulte [Web Application Firewall \(WAF\)](#).

## 1.2 Chamada de API

O WAF fornece as API Representational State Transfer (REST), permitindo que você use solicitações HTTPS para chamá-las. Para mais detalhes, consulte [Chamada de API](#).

## 1.3 Conceitos

- **Conta**

Uma conta é criada após o registro bem-sucedido. A conta tem permissões de acesso total para todos os seus serviços e recursos de nuvem. Ela pode ser usada para redefinir senhas de usuários e conceder permissões ao usuário. A conta é uma entidade de pagamento e não deve ser utilizada para realizar a gestão de rotina. Para fins de segurança, crie usuários do IAM e conceda a eles permissões para o gerenciamento de rotina.
- **Usuário**

Um usuário do IAM é criado por uma conta no IAM para usar os serviços em nuvem. Cada usuário do IAM tem suas próprias credenciais de identidade (senha e chaves de acesso).

- Região

As regiões são divididas com base na localização geográfica e na latência da rede. Serviços públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) e Image Management Service (IMS), são compartilhados na mesma região. As regiões são classificadas como regiões universais e regiões dedicadas. Uma região universal fornece serviços de nuvem universal para locatários comuns. Uma região dedicada fornece serviços do mesmo tipo apenas ou para locatários específicos.

# 2 Visão geral da API

Você pode usar todas as funções do WAF por meio das suas API.

<b>Tipo</b>	<b>Descrição</b>
As API do modo nuvem	As API para criar, modificar, consultar e remover nomes de domínio no modo nuvem.
As API de modo dedicado	As API para criar, modificar, consultar e remover nomes de domínio no modo dedicado
As API de certificados	As API para criação, modificação e consulta de certificados.
As API de regra de proteção	As API para criar, atualizar, consultar e excluir regras de proteção.
As API de política de proteção	As API para criar políticas em lotes e modificar os nomes de domínio aos quais uma política se aplica.
API do evento	API para consultar detalhes de um evento.
API de consulta de nome de domínio	API para consulta de nomes de domínio conectados ao WAF



# 3 Chamada de API

---

## 3.1 Criação de uma solicitação de API

Esta seção descreve a estrutura de uma solicitação de API REST e usa a API do IAM para **obtenção de um token de usuário** como exemplo para demonstrar como chamar uma API. O token obtido pode então ser usado para autenticar a chamada das outras API.

### URI de solicitação

Um URI de solicitação está no seguinte formato:

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

Embora um URI de solicitação esteja incluído no cabeçalho da solicitação, a maioria das linguagens de programação ou estruturas exigem que o URI de solicitação seja transmitido separadamente.

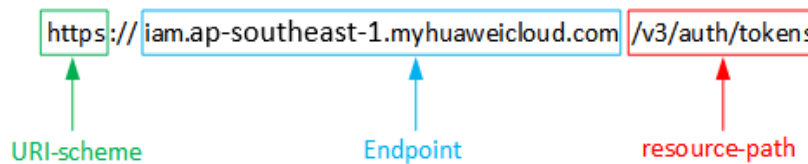
- **URI-scheme:**  
Protocolo usado para transmitir solicitações. Todas as API usam HTTPS.
- **Endpoint:**  
Nome de domínio ou endereço IP do servidor que possui o serviço REST. O endpoint varia entre serviços em diferentes regiões. Ele pode ser obtido em **Regiões e Endpoints**.  
Por exemplo, o endpoint do IAM na região **CN-Hong Kong** é **iam.ap-southeast-1.myhuaweicloud.com**.
- **resource-path:**  
Caminho de acesso de uma API para executar uma operação especificada. Obtenha o caminho a partir do URI de uma API. Por exemplo, o **resource-path** da API usada para obter um token de usuário é **/v3/auth/tokens**.
- **query-string:**  
Parâmetro de consulta, que é opcional. Verifique se um ponto de interrogação (?) está incluído antes de cada parâmetro de consulta no formato "Nome do parâmetro = valor do parâmetro". Por exemplo, **?limit=10** indica que um máximo de 10 registros de dados serão exibidos.

Por exemplo, para obter um token IAM na região **CN-Hong Kong**, obter o endpoint do IAM (iam.ap-southeast-1.myhuaweicloud.com) para essa região e o **resource-path** (**/v3/auth/**

**tokens**) no URI da API usada para **obter um token de usuário**. Em seguida, construa o URI da seguinte forma:

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

**Figura 3-1** Exemplo de URI



#### 📖 NOTA

Para simplificar a exibição de URI neste documento, cada API é fornecida apenas com um **resource-path** e um método de solicitação. O **URI-scheme** de todas as API é **HTTPS**, e os endpoints de todas as API na mesma região são idênticos.

## Métodos de solicitação

O protocolo HTTP define os seguintes métodos de solicitação que podem ser usados para enviar uma solicitação ao servidor:

- **GET**: solicita que o servidor retorne os recursos especificados.
- **PUT**: solicita que o servidor atualize os recursos especificados.
- **POST**: solicita que o servidor adicione recursos ou execute operações especiais.
- **DELETE**: solicita que o servidor exclua recursos especificados, por exemplo, um objeto.
- **HEAD**: O mesmo que GET, exceto que o servidor deve retornar apenas o cabeçalho da resposta.
- **PATCH**: solicita ao servidor que atualize o conteúdo parcial de um recurso especificado. Se o recurso não existir, um novo recurso será criado.

Por exemplo, no caso da API usada para **obter um token de usuário**, o método de solicitação é POST. A solicitação é o seguinte:

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

## Cabeçalho da solicitação

Você também pode adicionar campos de cabeçalho adicionais a uma solicitação, como os campos exigidos por um método URI ou HTTP especificado. Por exemplo, para solicitar as informações de autenticação, adicione **Content-type**, que especifica o tipo de corpo da solicitação.

Os campos comuns de cabeçalho de solicitação são os seguintes:

- **Content-Type**: especifica o tipo ou formato do corpo da solicitação. Este campo é obrigatório e seu valor padrão é **aplicação/json**. Outros valores deste campo serão fornecidos para as API específicas, se houver.
- **X-Auth-Token**: especifica um token de usuário apenas para autenticação de API baseada em token. O token de usuário é uma resposta à API usada para **obter um token de usuário**. Esta API é a única que não requer autenticação.

 **NOTA**

Além de oferecer suporte à autenticação baseada em token, as API também oferecem suporte à autenticação usando ID da chave de acesso/chave de acesso secreta (AK/SK). Durante a autenticação baseada em AK/SK, um SDK é usado para assinar a solicitação, e os campos de cabeçalho **Authorization** (informações de assinatura) e **X-Sdk-Date** (hora em que a solicitação é enviada) são adicionados automaticamente à solicitação.

Para obter mais informações, consulte [Autenticação baseada em AK/SK](#).

A API usada para [obter um token de usuário](#) não requer autenticação. Portanto, apenas o campo **Content-type** precisa ser adicionado às solicitações para chamar a API. Um exemplo de tais solicitações é o seguinte:

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

## Corpo da solicitação

O corpo de uma solicitação geralmente é enviado em um formato estruturado, conforme especificado no campo de cabeçalho **Content-Type**. O corpo da solicitação transfere o conteúdo, exceto o cabeçalho da solicitação.

O corpo da solicitação varia entre as API. Algumas API não exigem o corpo da solicitação, como as API solicitadas usando os métodos GET e DELETE.

No caso da API usada para [obter um token de usuário](#), os parâmetros da solicitação e a descrição do parâmetro podem ser obtidos da solicitação da API. O seguinte fornece um exemplo de solicitação com um corpo incluído. Defina **username** para o nome de um usuário, **domainname** para o nome da conta que o usuário pertence to, **\*\*\*\*\*** para a senha de login do usuário e **xxxxxxxxxxxxxxxxxxxx** para o nome do projeto. Você pode obter mais informações sobre projetos em [Regiões e Endpoints](#) Verifique o valor da coluna **Region**.

 **NOTA**

O parâmetro **scope** especifica onde um token entra em vigor. Você pode definir **scope** para uma conta ou um projeto em uma conta. No exemplo a seguir, o token tem efeito somente para os recursos em um projeto especificado. Para obter mais informações sobre essa API, consulte [Obtenção de um token de usuário](#).

```
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"
      }
    }
  }
}
```

```
}  
}
```

Se todos os dados necessários para a solicitação da API estiverem disponíveis, você poderá enviar a solicitação para chamar a API por meio de [curl](#), [Postman](#) ou coding. Na resposta à API usada para obter um token de usuário, **x-subject-token** é o token de usuário desejado. Esse token pode ser usado para autenticar a chamada de outras API.

## 3.2 Autenticação

As solicitações para chamar uma API podem ser autenticadas usando um dos seguintes métodos:

- Autenticação baseada em token: As solicitações são autenticadas usando um token.
- Autenticação baseada em AK/SK: As solicitações são autenticadas criptografando o corpo da solicitação usando um par AK/SK. Este método é recomendado porque fornece uma segurança mais alta do que a autenticação baseada em token.

### Autenticação baseada em token

#### NOTA

O período de validade de um token é de 24 horas. Ao usar um token para autenticação, armazene-o em cache para impedir a chamada freqüente da API do IAM usada para obter um token de usuário.

Um token especifica permissões temporárias em um sistema de computador. Durante a autenticação da API usando um token, o token é adicionado às solicitações para obter permissões para chamar a API.

O token pode ser obtido chamando a API necessária. Para obter mais informações, consulte [Obtenção de um token de usuário](#). Um token no nível do projeto é necessário para chamar essa API, ou seja, **auth.scope** deve ser definido como **project** no corpo da solicitação.

Exemplo:

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

Depois que um token é obtido, o campo de cabeçalho **X-Auth-Token** deve ser adicionado às solicitações para especificar o token ao chamar outras API. Por exemplo, se o token é

**ABCDEFJ..., X-Auth-Token: ABCDEFJ...** pode ser adicionado a uma solicitação da seguinte forma:

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

## Autenticação baseada em AK/SK

### NOTA

A autenticação baseada em AK/SK suporta solicitações de API com um corpo não maior que 12 MB. Para solicitações de API com um corpo maior, a autenticação baseada em token é recomendada.

Na autenticação baseada em AK/SK, AK/SK é usado para assinar solicitações e a assinatura é então adicionada às solicitações de autenticação.

- AK: ID da chave de acesso, que é um identificador exclusivo usado em conjunto com uma chave de acesso secreta para assinar solicitações criptograficamente.
- SK: chave de acesso secreta usada em conjunto com uma AK para assinar solicitações criptograficamente. Ele identifica um remetente da solicitação e impede que a solicitação seja modificada.

Na autenticação baseada em AK/SK, você pode usar um AK/SK para assinar solicitações com base no algoritmo de assinatura ou usar o SDK de assinatura para assinar solicitações. Para obter detalhes sobre como assinar solicitações e usar o SDK de assinatura, consulte [Guia de assinatura da API](#).

### AVISO

O SDK de assinatura é usado apenas para solicitações de assinatura e é diferente dos SDK fornecidos pelos serviços.

## 3.3 Resposta

### Código de status

Depois de enviar uma solicitação, você receberá uma resposta, incluindo um código de status, cabeçalho de resposta e corpo de resposta.

Um código de status é um grupo de dígitos, variando de 1xx a 5xx. Indica o status de uma solicitação. Para obter mais informações, consulte [Código de status](#).

Por exemplo, se o código de status **201** é retornado para chamar a API usada para [obter um token de usuário](#), a solicitação foi bem-sucedida.

### Cabeçalho de resposta

Semelhante a uma solicitação, uma resposta também tem um cabeçalho, por exemplo, **content-type**.

A seguir, mostra-se o cabeçalho de resposta da API para [obter um token de usuário](#), em que **x-subject-token** é o token de usuário desejado. Esse token pode ser usado para autenticar a chamada de outras API.

**Figura 3-2** Campos de cabeçalho da resposta à solicitação para obter um token de usuário

```

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
→ MIIYXQYJKoZIhvcNAQcCoIIYTCCEoCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOensiZXhwaXJlc19hdCI6IiwMTktMDItMTNUMD
fj3KJs6YgKnPvNRbW2eZ5eb78SZOkajACgkIQ01wi4JIGzrpd18LGXK5bdfq4lqHCYb8P4NaYONVejcAgzJVeFYtLWT1GSO0zxKZmlQHq82HBqHdgIZO9fuEbL5dMhdavj+33wEI
xHRC9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXl1jipPEGA270g1FruooL6jggIFkNPQuFSOU8+uSsttVwrNfsC+qT22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUUVhVpxk8pxiX1wTEboX-
RzT6MUbpvGw-oPNFYxjECKnoH3HRozv0vN--n5d6Nbxg==

x-xss-protection → 1; mode=block;

```

### (Opcional) Corpo de resposta

O corpo de uma resposta geralmente é retornado em formato estruturado, conforme especificado no campo de cabeçalho **Content-Type**. O corpo da resposta transfere o conteúdo, exceto o cabeçalho da resposta.

A seguir, mostramos parte do corpo da resposta da API para **obter um token de usuário**. Por uma questão de espaço, apenas parte do conteúdo é exibido aqui.

```

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

```

Se ocorrer um erro durante a chamada da API, um código de erro e uma mensagem serão exibidos. O seguinte mostra um corpo de resposta de erro.

```

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

```

No corpo da resposta, **error\_code** é um código de erro e **error\_msg** fornece informações sobre o erro.

# 4 API

## 4.1 Gerenciamento de sites protegidos no modo nuvem

### 4.1.1 Essa API é usada para consultar a lista de nomes de domínio protegidos no modo nuvem.

#### Função

Essa API é usada para consultar a lista de nomes de domínio protegidos no modo nuvem.

#### URI

GET /v1/{project\_id}/waf/instance

**Tabela 4-1** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

**Tabela 4-2** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.
page	Não	Integer	Número de página dos dados a serem retornados durante a consulta de paginação. O valor padrão é <b>1</b> , indicando que os dados na primeira página são retornados. Padrão: <b>1</b>
pagesize	Não	Integer	Número de resultados em cada página durante a consulta de paginação. Faixa de valor: <b>1 a 100</b> . O valor padrão é <b>10</b> , indicando que cada página contém 10 resultados. Padrão: <b>10</b>
hostname	Não	String	O nome de domínio cujas informações você deseja consultar. Esse parâmetro é usado para consultar informações sobre um nome de domínio especificado. Se esse parâmetro não for especificado, todos os nomes de domínio protegidos com o WAF da nuvem serão consultados.
policyname	Não	String	Nome da política de proteção. Este parâmetro é utilizado para consultar nomes de domínio adicionados a uma política de proteção especificada. Este parâmetro é opcional.

## Parâmetros de solicitação

**Tabela 4-3** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).



Parâmetro	Obrigatório	Tipo	Descrição
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/ json;charset=utf8</b>

## Parâmetros de resposta

Código de estado: 200

Tabela 4-4 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	Número de nomes de domínio protegidos com o WAF na nuvem
items	Array of <b>CloudWafHostItem</b> objects	Matriz de detalhes sobre os nomes de domínio protegidos com o WAF na nuvem.

Tabela 4-5 CloudWafHostItem

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostid	String	ID do nome de domínio
region	String	ID da região. Esse parâmetro é incluído quando o nome de domínio é adicionado ao WAF por meio do console. Esse parâmetro é deixado em branco quando o nome de domínio é adicionado ao WAF ao chamar uma API. Você pode consultar o ID da região na página Regiões e Endpoints no site da Huawei Cloud.
description	String	(Opcional) Descrições dos nomes de domínio
type	Integer	Modo de implantação do WAF. O valor padrão é 1. Atualmente, apenas o proxy reverso é suportado. Este parâmetro é redundante.
proxy	Boolean	Se um proxy é usado para o nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>false</b>: Nenhum proxy é usado.</li> <li>● <b>true</b>: Um proxy é usado.</li> </ul>
hostname	String	Nome de domínio adicionado ao WAF na nuvem.
access_code	String	Prefixo CNAME

Parâmetro	Tipo	Descrição
policyid	String	ID da política
timestamp	Long	Hora em que o nome de domínio foi adicionado ao WAF.
protect_status	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>
access_status	Integer	Status de acesso ao nome de domínio. O valor pode ser <b>0</b> ou <b>1</b> . <b>0</b> : O tráfego do site não foi encaminhado para o WAF. <b>1</b> : O tráfego do site foi encaminhado para o WAF.
exclusive_ip	Boolean	Se usar um endereço IP dedicado. <ul style="list-style-type: none"> <li>● <b>true</b>: Use um endereço IP dedicado.</li> <li>● <b>false</b>: Não use um endereço IP dedicado.</li> </ul>
paid_type	String	Modo pago. Atualmente, apenas o modo pré-pago é suportado. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>prePaid</b></li> </ul>
web_tag	String	Nome do site, que é o mesmo que o nome do site nos detalhes do nome de domínio no console do WAF.
flag	<b>Flag</b> object	Identificador especial, que é usado no console.

Tabela 4-6 Flag

Parâmetro	Tipo	Descrição
pci_3ds	String	Se o site passa a verificação de certificação PCI 3DS. <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI 3DS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação do PCI 3DS.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
pci_dss	String	Se o site passou na verificação de certificação PCI DSS. <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI DSS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação PCI DSS.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cname	String	O registro CNAME que está sendo usado. <ul style="list-style-type: none"> <li>● <b>old</b>: O registro CNAME antigo é usado.</li> <li>● <b>new</b>: O novo registro CNAME é usado.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>old</b></li> <li>● <b>new</b></li> </ul>
is_dual_az	String	Se o WAF suporta o Multi-AZ DR <ul style="list-style-type: none"> <li>● <b>true</b>: O WAF suporta DR multi-AZ.</li> <li>● <b>false</b>: O WAF não suporta DR multi-AZ.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ipv6	String	Se a proteção IPv6 é suportada. <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

**Código de estado: 400**

**Tabela 4-7** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-8** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-9** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**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-4",
    "hostname" : "www.demo.com",
    "access_code" : "7d06456ffaxxxxxxxxxxxx281bc13b",
    "policyid" : "bb2124fabe6f42ff9fe4770eeccb2670",
    "timestamp" : 1642648030687,
    "protect_status" : 1,
    "access_status" : 0,
    "exclusive_ip" : false,
    "web_tag" : "iii",
    "paid_type" : "prePaid"
  } ]
}
```

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.1.2 Adição de um nome de domínio ao Cloud WAF

#### Função

Essa API é usada para adicionar um nome de domínio ao WAF da nuvem.

#### URI

POST /v1/{project\_id}/waf/instance

**Tabela 4-10** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

**Tabela 4-11** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-12** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-13** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
hostname	Sim	String	O nome de domínio pode conter um máximo de 64 caracteres. Somente letras, dígitos, hífens, ( _ ), de sublinhados e pontos ( . ) são permitidos, por exemplo www.domain.com.
policyid	Não	String	ID da política usada inicialmente para o nome de domínio. Você pode chamar a API <b>ListPolicy</b> para consultar a lista de políticas e exibir o ID da política específica.
server	Sim	Array of <b>CloudWafServer</b> objects	Configuração do servidor de origem do nome de domínio protegido
certificateid	Não	String	ID do certificado. Ele pode ser obtido chamando a API <b>ListCertificates</b> . <ul style="list-style-type: none"> <li>● Este parâmetro não é necessário quando o protocolo do cliente é HTTP.</li> <li>● Este parâmetro é obrigatório quando o protocolo do cliente é HTTPS.</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
certificatename	Não	String	Nome do certificado. <ul style="list-style-type: none"> <li>● Este parâmetro não é necessário quando o protocolo do cliente é HTTP.</li> <li>● Este parâmetro é obrigatório quando o protocolo do cliente é HTTPS.</li> </ul>
web_tag	Não	String	Nome do site
exclusive_ip	Não	Boolean	Se usar um endereço IP dedicado. <ul style="list-style-type: none"> <li>● <b>true</b>: Use um endereço IP dedicado.</li> <li>● <b>false</b>: Não use um endereço IP dedicado.</li> </ul>
paid_type	Não	String	Modo de pagamento baseado em pacote. Atualmente, apenas o modo pré-pago é suportado.
proxy	Sim	Boolean	Se um proxy é usado para o nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>false</b>: Nenhum proxy é usado.</li> <li>● <b>true</b>: Um proxy é usado.</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
lb_algorithm	Não	String	<p>Algoritmos de balanceamento de carga. Este parâmetro está incluído apenas na edição profissional (antiga edição empresarial) e edição platina (antiga edição premium).</p> <ul style="list-style-type: none"> <li>● <b>Source IP hash:</b> As solicitações de um determinado endereço IP são encaminhadas para o mesmo servidor.</li> <li>● <b>Weighted round robin:</b> Todas as solicitações são distribuídas aos servidores de origem, por sua vez, com base no peso atribuído a cada servidor.</li> <li>● <b>Session hash:</b> Solicitações com um ID de sessão específico são encaminhadas para o mesmo servidor de origem. Certifique-se de que os identificadores de tráfego para fontes de ataque conhecidas estejam configurados depois que o nome de domínio foi adicionado ao WAF. Caso contrário, a configuração de hash da sessão não terá efeito.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>ip_hash</b></li> <li>● <b>round_robin</b></li> <li>● <b>session_hash</b></li> </ul>
description	Não	String	Descrição do nome de domínio

Tabela 4-14 CloudWafServer

Parâmetro	Obrigatório	Tipo	Descrição
front_protocol	Sim	String	<p>Protocolo usado pelo cliente para solicitar acesso ao servidor de origem.</p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>HTTP</b></li> <li>● <b>HTTPS</b></li> </ul>



Parâmetro	Obrigatório	Tipo	Descrição
back_protocol	Sim	String	Protocolo usado pelo WAF para encaminhar solicitações de clientes recebidas aos servidores de origem Valores de enumeração: <ul style="list-style-type: none"> <li>● HTTP</li> <li>● HTTPS</li> </ul>
weight	Não	Integer	Peso do servidor de origem. O algoritmo de balanceamento de carga encaminha solicitações para o servidor de origem com base no peso. O valor padrão é 1. Este campo não é incluído pelo WAF na nuvem.
address	Sim	String	Endereço IP do servidor de origem solicitado pelo cliente
port	Sim	Integer	Porta usada pelo WAF para encaminhar solicitações de clientes para o servidor de origem
type	Sim	String	Formato de endereço IP do servidor de origem, IPv4 e IPv6 Valores de enumeração: <ul style="list-style-type: none"> <li>● ipv4</li> <li>● ipv6</li> </ul>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-15** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio adicionado ao WAF na nuvem.
policyid	String	ID da política
access_code	String	Prefixo CNAME

Parâmetro	Tipo	Descrição
protect_status	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>
access_status	Integer	Status de acesso ao nome de domínio. O valor pode ser <b>0</b> ou <b>1</b> . <b>0</b> : O tráfego do site não foi encaminhado para o WAF. <b>1</b> : O tráfego do site foi encaminhado para o WAF.
lb_algorithm	String	Algoritmos de balanceamento de carga. Este parâmetro está incluído apenas na edição profissional (antiga edição empresarial) e edição platina (antiga edição premium). <ul style="list-style-type: none"> <li>● <b>Source IP hash</b>: As solicitações de um determinado endereço IP são encaminhadas para o mesmo servidor.</li> <li>● <b>Weighted round robin</b>: Todas as solicitações são distribuídas aos servidores de origem, por sua vez, com base no peso atribuído a cada servidor.</li> <li>● <b>Session hash</b>: Solicitações com um ID de sessão específico são encaminhadas para o mesmo servidor de origem. Certifique-se de que os identificadores de tráfego para fontes de ataque conhecidas estejam configurados depois que o nome de domínio foi adicionado ao WAF. Caso contrário, a configuração de hash da sessão não terá efeito.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>ip_hash</b></li> <li>● <b>round_robin</b></li> <li>● <b>session_hash</b></li> </ul>
protocol	String	Tipo de protocolo de cliente retornado
certificateid	String	ID do certificado devolvido
certificatename	String	Nome do certificado
server	Array of <b>CloudWafServer</b> objects	Configuração do servidor de origem do nome de domínio protegido

Parâmetro	Tipo	Descrição
proxy	Boolean	Se um proxy é usado para o nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>false</b>: Nenhum proxy é usado.</li> <li>● <b>true</b>: Um proxy é usado.</li> </ul>
timestamp	Long	Hora em que o nome de domínio foi adicionado ao WAF.
exclusive_ip	Boolean	Se usar um endereço IP dedicado. <ul style="list-style-type: none"> <li>● <b>true</b>: Use um endereço IP dedicado.</li> <li>● <b>false</b>: Não use um endereço IP dedicado.</li> </ul>
web_tag	String	Nome do site
http2_enable	Boolean	Suportar ou não HTTP/2. <ul style="list-style-type: none"> <li>● <b>true</b>: HTTP/2 é suportado.</li> <li>● <b>false</b>: HTTP/2 não é suportado.</li> </ul>
block_page	<b>BlockPage</b> object	Configuração da página de alarme
flag	<b>Flag</b> object	Identificador especial, que é usado no console.
extend	Map<String,String>	Campo estendido, que é usado para salvar algumas informações de configuração sobre o nome de domínio protegido.

**Tabela 4-16** CloudWafServer

Parâmetro	Tipo	Descrição
front_protocol	String	Protocolo usado pelo cliente para solicitar acesso ao servidor de origem. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>HTTP</b></li> <li>● <b>HTTPS</b></li> </ul>
back_protocol	String	Protocolo usado pelo WAF para encaminhar solicitações de clientes recebidas aos servidores de origem Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>HTTP</b></li> <li>● <b>HTTPS</b></li> </ul>

Parâmetro	Tipo	Descrição
weight	Integer	Peso do servidor de origem. O algoritmo de balanceamento de carga encaminha solicitações para o servidor de origem com base no peso. O valor padrão é <b>1</b> . Este campo não é incluído pelo WAF na nuvem.
address	String	Endereço IP do servidor de origem solicitado pelo cliente
port	Integer	Porta usada pelo WAF para encaminhar solicitações de clientes para o servidor de origem
type	String	Formato de endereço IP do servidor de origem, IPv4 e IPv6 Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>ipv4</b></li> <li>● <b>ipv6</b></li> </ul>

**Tabela 4-17** BlockPage

Parâmetro	Tipo	Descrição
template	String	Nome do modelo
custom_page	<b>CustomPage</b> object	Página de alarme personalizada
redirect_url	String	URL da página redirecionada

**Tabela 4-18** CustomPage

Parâmetro	Tipo	Descrição
status_code	String	Códigos de status
content_type	String	O tipo de conteúdo da página de alarme personalizada. O valor pode ser <b>text/html</b> , <b>text/xml</b> , ou <b>application/json</b> .
content	String	O conteúdo da página com base no tipo de página selecionado. Para obter detalhes, consulte o <i>Guia de usuário do Web Application Firewall (WAF)</i> .

**Tabela 4-19** Bandeira

Parâmetro	Tipo	Descrição
pci_3ds	String	<p>Se o site passa a verificação de certificação PCI 3DS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI 3DS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação do PCI 3DS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
pci_dss	String	<p>Se o site passou na verificação de certificação PCI DSS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI DSS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação PCI DSS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cname	String	<p>O registro CNAME que está sendo usado.</p> <ul style="list-style-type: none"> <li>● <b>old</b>: O registro CNAME antigo é usado.</li> <li>● <b>new</b>: O novo registro CNAME é usado.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>old</b></li> <li>● <b>new</b></li> </ul>
is_dual_az	String	<p>Se o WAF suporta o Multi-AZ DR</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O WAF suporta DR multi-AZ.</li> <li>● <b>false</b>: O WAF não suporta DR multi-AZ.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ipv6	String	<p>Se a proteção IPv6 é suportada.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

**Código de estado: 400**

**Tabela 4-20** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-21** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-22** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

```
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
}
```

## Exemplo de respostas

**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" : "41cba8aee2e94bcd5f57460874205494",
  "domainid" : "d4ecb00b031941ce9171b7bc3386883f",
  "projectid" : "0456cf04d6f64725ab02ed5bd2efdfa4",
  "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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.1.3 Consulta de detalhes sobre um nome de domínio por ID de nome de domínio no modo nuvem

### Função

Consulta de detalhes sobre um nome de domínio por ID de nome de domínio no modo nuvem

### URI

GET /v1/{project\_id}/waf/instance/{instance\_id}

**Tabela 4-23** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
instance_id	Sim	String	ID do nome de domínio. Ele pode ser obtido chamando a API <b>ListHost</b> .

**Tabela 4-24** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

### Parâmetros de solicitação

**Tabela 4-25** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).



Parâmetro	Obrigatório	Tipo	Descrição
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json; charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-26** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio adicionado ao WAF na nuvem.
policyid	String	ID da política usada para o nome de domínio.
domainid	String	ID da conta, que é o mesmo que o ID da conta na página <b>My Credentials</b> . Para acessar esta página, faça login no console de gerenciamento do Huawei Cloud, passe o cursor sobre seu nome de usuário e clique em <b>My Credentials</b> na janela exibida.
projectid	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
enterprise_project_id	String	ID do projeto empresarial. Para obter a ID, faça login primeiro no console de gerenciamento do Huawei Cloud. Na barra de menus na parte superior da página, escolha <b>Enterprise &gt; Project Management</b> . Em seguida, clique no nome do projeto e visualize o ID.
protocol	String	Tipo de protocolo backend. O valor pode ser HTTPS, HTTP ou HTTP&HTTPS.
server	Array of <b>CloudWafServer</b> objects	Configuração do servidor de origem do nome de domínio protegido
proxy	Boolean	Se um proxy é usado para o nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>false</b>: Nenhum proxy é usado.</li> <li>● <b>true</b>: Um proxy é usado.</li> </ul>

Parâmetro	Tipo	Descrição
protect_status	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>
access_status	Integer	Status de acesso ao nome de domínio. O valor pode ser <b>0</b> ou <b>1</b> . <b>0</b> : O tráfego do site não foi encaminhado para o WAF. <b>1</b> : O tráfego do site foi encaminhado para o WAF.
access_code	String	Prefixo CNAME
locked	Integer	Este parâmetro é reservado, que será usado para congelar um nome de domínio.
timestamp	Long	Timestamp (ms) quando o nome de domínio protegido é criado.
certificateid	String	ID do certificado HTTPS.
certificatename	String	Nome do certificado
tls	String	Versão mínima do TLS. O valor pode ser <b>TLS v1.0</b> , <b>TLS v1.1</b> , ou <b>TLS v1.2</b> . O TLS v1.0 é usado por padrão. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>TLS v1.0</b></li> <li>● <b>TLS v1.1</b></li> <li>● <b>TLS v1.2</b></li> <li>● <b>TLS v1.3</b></li> </ul>

Parâmetro	Tipo	Descrição
cipher	String	<p>Suíte Cipher. O valor pode ser <b>cipher_1</b>, <b>cipher_2</b>, <b>cipher_3</b>, <b>cipher_4</b>, ou <b>cipher_default</b>: <b>cipher_1</b>: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH</p> <ul style="list-style-type: none"> <li>● <b>cipher_2</b>: ECDH+AESGCM:EDH+AESGCM</li> <li>● <b>cipher_3</b>: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH</li> <li>● <b>cipher_4</b>: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH</li> <li>● <b>cipher_default</b>: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>cipher_1</b></li> <li>● <b>cipher_2</b></li> <li>● <b>cipher_3</b></li> <li>● <b>cipher_4</b></li> <li>● <b>cipher_default</b></li> </ul>
block_page	<b>BlockPage</b> object	Configuração da página de alarme
extend	Map<String,String>	Campo estendido, que é usado para salvar algumas informações de configuração sobre o nome de domínio protegido.
traffic_mark	<b>TrafficMark</b> object	Identificador de tráfego
circuit_breaker	<b>CircuitBreaker</b> object	Configuração do disjuntor

Parâmetro	Tipo	Descrição
lb_algorithm	String	<p>Algoritmos de balanceamento de carga. Este parâmetro está incluído apenas na edição profissional (antiga edição empresarial) e edição platina (antiga edição premium).</p> <ul style="list-style-type: none"> <li>● <b>Source IP hash:</b> As solicitações de um determinado endereço IP são encaminhadas para o mesmo servidor.</li> <li>● <b>Weighted round robin:</b> Todas as solicitações são distribuídas aos servidores de origem, por sua vez, com base no peso atribuído a cada servidor.</li> <li>● <b>Session hash:</b> Solicitações com um ID de sessão específico são encaminhadas para o mesmo servidor de origem. Certifique-se de que os identificadores de tráfego para fontes de ataque conhecidas estejam configurados depois que o nome de domínio foi adicionado ao WAF. Caso contrário, a configuração de hash da sessão não terá efeito.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>ip_hash</b></li> <li>● <b>round_robin</b></li> <li>● <b>session_hash</b></li> </ul>
timeout_config	<b>TimeoutConfig</b> object	Configurações de tempo limite
web_tag	String	Nome do site
flag	<b>Flag</b> object	Identificador especial, que é usado no console.
description	String	Observações do site
http2_enable	Boolean	<p>Suportar ou não HTTP/2.</p> <ul style="list-style-type: none"> <li>● <b>true:</b> HTTP/2 é suportado.</li> <li>● <b>false:</b> HTTP/2 não é suportado.</li> </ul>
exclusive_ip	Boolean	<p>Se usar um endereço IP dedicado.</p> <ul style="list-style-type: none"> <li>● <b>true:</b> Use um endereço IP dedicado.</li> <li>● <b>false:</b> Não use um endereço IP dedicado.</li> </ul>
access_progress	Array of <b>Access_progress</b> objects	Progresso do acesso, que é usado apenas para o novo console do WAF.

**Tabela 4-27** CloudWafServer

Parâmetro	Tipo	Descrição
front_protocol	String	Protocolo usado pelo cliente para solicitar acesso ao servidor de origem. Valores de enumeração: <ul style="list-style-type: none"> <li>● HTTP</li> <li>● HTTPS</li> </ul>
back_protocol	String	Protocolo usado pelo WAF para encaminhar solicitações de clientes recebidas aos servidores de origem Valores de enumeração: <ul style="list-style-type: none"> <li>● HTTP</li> <li>● HTTPS</li> </ul>
weight	Integer	Peso do servidor de origem. O algoritmo de balanceamento de carga encaminha solicitações para o servidor de origem com base no peso. O valor padrão é 1. Este campo não é incluído pelo WAF na nuvem.
address	String	Endereço IP do servidor de origem solicitado pelo cliente
port	Integer	Porta usada pelo WAF para encaminhar solicitações de clientes para o servidor de origem
type	String	Formato de endereço IP do servidor de origem, IPv4 e IPv6 Valores de enumeração: <ul style="list-style-type: none"> <li>● ipv4</li> <li>● ipv6</li> </ul>

**Tabela 4-28** BlockPage

Parâmetro	Tipo	Descrição
template	String	Nome do modelo
custom_page	<b>CustomPage</b> object	Página de alarme personalizada
redirect_url	String	URL da página redirecionada

**Tabela 4-29** CustomPage

Parâmetro	Tipo	Descrição
status_code	String	Códigos de status
content_type	String	O tipo de conteúdo da página de alarme personalizada. O valor pode ser <b>text/html</b> , <b>text/xml</b> , ou <b>application/json</b> .
content	String	O conteúdo da página com base no tipo de página selecionado. Para obter detalhes, consulte o <i>Guia de usuário do Web Application Firewall (WAF)</i> .

**Tabela 4-30** TrafficMark

Parâmetro	Tipo	Descrição
sip	Array of strings	Etiqueta IP. Campo do cabeçalho da solicitação HTTP do endereço IP original do cliente.
cookie	String	Tag da sessão. Essa tag é usada por regras de origem de ataque conhecidas para bloquear ataques maliciosos com base em atributos de cookies. Esse parâmetro deve ser configurado em regras de origem de ataque conhecidas para bloquear solicitações com base em atributos de cookie.
params	String	Tag do usuário. Essa tag é usada por regras de origem de ataque conhecidas para bloquear ataques maliciosos com base em atributos de params. Esse parâmetro deve ser configurado para bloquear solicitações com base nos atributos params.

**Tabela 4-31** CircuitBreaker

Parâmetro	Tipo	Descrição
switch	Boolean	Se deve ativar a proteção de conexão. <ul style="list-style-type: none"> <li>● <b>true</b>: Ative a proteção de conexão.</li> <li>● <b>false</b>: Desative a proteção de conexão.</li> </ul>
dead_num	Integer	Limite de erro 502/504. 502/504 erros permitidos a cada 30 segundos.
dead_ratio	Number	Uma proteção contra avarias é acionada quando o limite de erro 502/504 e o limite percentual foram atingidos.

Parâmetro	Tipo	Descrição
block_time	Integer	Período de proteção após a primeira quebra. Durante esse período, o WAF deixa de encaminhar solicitações de clientes.
superposition_num	Integer	O multiplicador máximo que você pode usar para quebras consecutivas. O número de avarias é contado a partir de 0 sempre que a duração da proteção contra avarias acumulada atinge 3.600s. Por exemplo, suponha que o Tempo de Inatividade Inicial (s) esteja definido como 180s e <b>Multiplier for Consecutive Breakdowns</b> esteja definido como 3. Se a avaria for acionada pela segunda vez, ou seja, menos de 3, a duração da proteção é de 360s (180s X 2). Se a avaria for acionada pelo terceiro ou quarto tempo, ou seja, igual ou superior a 3, a duração da proteção é de 540s (180s X 3). Quando a duração do tempo de inatividade acumulado excede 1 hora (3.600s), o número de avarias é contado a partir de 0.
suspend_num	Integer	Limite do número de solicitações de URL pendentes. A proteção de conexão é acionada quando o limite é atingido.
sus_block_time	Integer	Duração do tempo de inatividade após a proteção da conexão ser acionada. Durante esse período, o WAF deixa de encaminhar solicitações de sites.

**Tabela 4-32** TimeoutConfig

Parâmetro	Tipo	Descrição
connect_timeout	Integer	Tempo limite para o WAF se conectar ao servidor de origem.
send_timeout	Integer	Tempo limite para o WAF enviar solicitações ao servidor de origem.
read_timeout	Integer	Tempo limite para o WAF receber respostas do servidor de origem.

**Tabela 4-33** Bandeira

Parâmetro	Tipo	Descrição
pci_3ds	String	<p>Se o site passa a verificação de certificação PCI 3DS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI 3DS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação do PCI 3DS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
pci_dss	String	<p>Se o site passou na verificação de certificação PCI DSS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI DSS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação PCI DSS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cname	String	<p>O registro CNAME que está sendo usado.</p> <ul style="list-style-type: none"> <li>● <b>old</b>: O registro CNAME antigo é usado.</li> <li>● <b>new</b>: O novo registro CNAME é usado.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>old</b></li> <li>● <b>new</b></li> </ul>
is_dual_az	String	<p>Se o WAF suporta o Multi-AZ DR</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O WAF suporta DR multi-AZ.</li> <li>● <b>false</b>: O WAF não suporta DR multi-AZ.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ipv6	String	<p>Se a proteção IPv6 é suportada.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>



**Tabela 4-34** Access\_progress

Parâmetro	Tipo	Descrição
step	Integer	Etapa
status	Integer	Estado. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: O passo não foi concluído.</li> <li>● <b>1</b>: O passo terminou.</li> </ul>

**Código de estado: 400**

**Tabela 4-35** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-36** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-37** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

OK

```
{
  "id" : "31af669f567246c289771694f2112289",
  "hostname" : "www.demo.com",
  "protocol" : "HTTP",
  "server" : [ {
    "address" : "x.x.x.x",
    "port" : 80,
    "type" : "ipv4",
    "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" : "0456cf04d6f64725ab02ed5bd2efd4",
  "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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.1.4 Atualização de configurações de nomes de domínio protegidos com o Cloud WAF

### Função

Essa API é usada para atualizar configurações de nomes de domínio protegidos com o WAF na nuvem. As novas informações do servidor de origem substituirão as informações do servidor de origem antigo. Se você quiser manter as informações antigas, forneça-as como dados novos. Você pode fornecer apenas as informações atualizadas no corpo da solicitação.

### URI

PATCH /v1/{project\_id}/waf/instance/{instance\_id}

Tabela 4-38 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
instance_id	Sim	String	ID do nome de domínio. Ele pode ser obtido chamando a API <b>ListHost</b> .

Tabela 4-39 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-40** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-41** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
proxy	Não	Boolean	Se um proxy é usado para o nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>false</b>: Nenhum proxy é usado.</li> <li>● <b>true</b>: Um proxy é usado.</li> </ul>
certificateid	Não	String	ID do certificado. Ele pode ser obtido chamando a API <b>ListCertificates</b> . <ul style="list-style-type: none"> <li>● Este parâmetro não é necessário quando o protocolo do cliente é HTTP.</li> <li>● Este parâmetro é obrigatório quando o protocolo do cliente é HTTPS.</li> </ul>
certificatename	Não	String	Nome do certificado. <ul style="list-style-type: none"> <li>● Este parâmetro não é necessário quando o protocolo do cliente é HTTP.</li> <li>● Este parâmetro é obrigatório quando o protocolo do cliente é HTTPS.</li> </ul>
server	Não	Array of <b>CloudWafServer</b> objects	Configuração do servidor de origem do nome de domínio protegido

Parâmetro	Obrigatório	Tipo	Descrição
tls	Não	String	<p>Versão mínima do TLS. O valor pode ser <b>TLS v1.0</b>, <b>TLS v1.1</b>, ou <b>TLS v1.2</b>. O TLS v1.0 é usado por padrão.</p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"><li>● <b>TLS v1.0</b></li><li>● <b>TLS v1.1</b></li><li>● <b>TLS v1.2</b></li><li>● <b>TLS v1.3</b></li></ul>

Parâmetro	Obrigatório	Tipo	Descrição
cipher	Não	String	<p>Suíte Cipher. O valor pode ser <b>cipher_1</b>, <b>cipher_2</b>, <b>cipher_3</b>, <b>cipher_4</b>, ou <b>cipher_default</b>:</p> <p><b>cipher_1</b>: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH</p> <ul style="list-style-type: none"> <li>● <b>cipher_2</b>: ECDH +AESGCM:EDH+AESGCM</li> <li>● <b>cipher_3</b>: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH</li> <li>● <b>cipher_4</b>: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH</li> <li>● <b>cipher_default</b>: The cryptographic algorithms are ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>cipher_1</b></li> <li>● <b>cipher_2</b></li> <li>● <b>cipher_3</b></li> <li>● <b>cipher_4</b></li> <li>● <b>cipher_default</b></li> </ul>
http2_enable	Não	Boolean	<p>Suportar ou não HTTP/2.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: HTTP/2 é suportado.</li> <li>● <b>false</b>: HTTP/2 não é suportado.</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
ipv6_enable	Não	Boolean	Se deve ativar a proteção IPv6. Somente a edição profissional (anteriormente Enterprise Edition) e a edição platina (anteriormente Premium Edition) suportam a proteção IPv6. <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 está ativada.</li> <li>● <b>false</b>: A proteção IPv6 está desativada.</li> </ul>
web_tag	Não	String	Nome do site
exclusive_ip	Não	Boolean	Se usar um endereço IP exclusivo. <ul style="list-style-type: none"> <li>● <b>true</b>: O endereço IP exclusivo é usado.</li> <li>● <b>false</b>: O endereço IP exclusivo não é prático.</li> </ul>
paid_type	Não	String	Modo de pagamento do pacote. Atualmente, apenas o modo pré-pago é suportado.
block_page	Não	<b>BlockPage</b> object	Configuração da página de alarme
traffic_mark	Não	<b>TrafficMark</b> object	Identificador de tráfego
flag	Não	<b>Flag</b> object	Identificador especial, que é usado no console.
extend	Não	Map<String,String>	Campo estendido, que é usado para salvar algumas informações de configuração sobre o nome de domínio protegido.
circuit_breaker	Não	<b>CircuitBreaker</b> object	Configuração do disjuntor
timeout_config	Não	<b>TimeoutConfig</b> object	Configurações de tempo limite

**Tabela 4-42** CloudWafServer

Parâmetro	Obrigatório	Tipo	Descrição
front_protocol	Sim	String	Protocolo usado pelo cliente para solicitar acesso ao servidor de origem. Valores de enumeração: <ul style="list-style-type: none"> <li>● HTTP</li> <li>● HTTPS</li> </ul>
back_protocol	Sim	String	Protocolo usado pelo WAF para encaminhar solicitações de clientes recebidas aos servidores de origem Valores de enumeração: <ul style="list-style-type: none"> <li>● HTTP</li> <li>● HTTPS</li> </ul>
weight	Não	Integer	Peso do servidor de origem. O algoritmo de balanceamento de carga encaminha solicitações para o servidor de origem com base no peso. O valor padrão é 1. Este campo não é incluído pelo WAF na nuvem.
address	Sim	String	Endereço IP do servidor de origem solicitado pelo cliente
port	Sim	Integer	Porta usada pelo WAF para encaminhar solicitações de clientes para o servidor de origem
type	Sim	String	Formato de endereço IP do servidor de origem, IPv4 e IPv6 Valores de enumeração: <ul style="list-style-type: none"> <li>● ipv4</li> <li>● ipv6</li> </ul>

**Tabela 4-43** BlockPage

Parâmetro	Obrigatório	Tipo	Descrição
template	Sim	String	Nome do modelo
custom_page	Não	<b>CustomPage</b> object	Página de alarme personalizada
redirect_url	Não	String	URL da página redirecionada



**Tabela 4-44** CustomPage

Parâmetro	Obrigatório	Tipo	Descrição
status_code	Sim	String	Códigos de status
content_type	Sim	String	O tipo de conteúdo da página de alarme personalizada. O valor pode ser <b>text/html</b> , <b>text/xml</b> , ou <b>application/json</b> .
content	Sim	String	O conteúdo da página com base no tipo de página selecionado. Para obter detalhes, consulte o <i>Guia de usuário do Web Application Firewall (WAF)</i> .

**Tabela 4-45** TrafficMark

Parâmetro	Obrigatório	Tipo	Descrição
sip	Não	Array of strings	Etiqueta IP. Campo do cabeçalho da solicitação HTTP do endereço IP original do cliente.
cookie	Não	String	Tag da sessão. Essa tag é usada por regras de origem de ataque conhecidas para bloquear ataques maliciosos com base em atributos de cookies. Esse parâmetro deve ser configurado em regras de origem de ataque conhecidas para bloquear solicitações com base em atributos de cookie.
params	Não	String	Tag do usuário. Essa tag é usada por regras de origem de ataque conhecidas para bloquear ataques maliciosos com base em atributos de params. Esse parâmetro deve ser configurado para bloquear solicitações com base nos atributos params.

**Tabela 4-46** Flag

Parâmetro	Obrigatório	Tipo	Descrição
pci_3ds	Não	String	<p>Se o site passa a verificação de certificação PCI 3DS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI 3DS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação do PCI 3DS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
pci_dss	Não	String	<p>Se o site passou na verificação de certificação PCI DSS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI DSS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação PCI DSS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cname	Não	String	<p>O registro CNAME que está sendo usado.</p> <ul style="list-style-type: none"> <li>● <b>old</b>: O registro CNAME antigo é usado.</li> <li>● <b>new</b>: O novo registro CNAME é usado.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>old</b></li> <li>● <b>new</b></li> </ul>
is_dual_az	Não	String	<p>Se o WAF suporta o Multi-AZ DR</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O WAF suporta DR multi-AZ.</li> <li>● <b>false</b>: O WAF não suporta DR multi-AZ.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
ipv6	Não	String	<p>Se a proteção IPv6 é suportada.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

**Tabela 4-47** CircuitBreaker

Parâmetro	Obrigatório	Tipo	Descrição
switch	Não	Boolean	<p>Se deve ativar a proteção de conexão.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: Ative a proteção de conexão.</li> <li>● <b>false</b>: Desative a proteção de conexão.</li> </ul>
dead_num	Não	Integer	Limite de erro 502/504. 502/504 erros permitidos a cada 30 segundos.
dead_ratio	Não	Number	Uma proteção contra avarias é acionada quando o limite de erro 502/504 e o limite percentual foram atingidos.
block_time	Não	Integer	Período de proteção após a primeira quebra. Durante esse período, o WAF deixa de encaminhar solicitações de clientes.

Parâmetro	Obrigatório	Tipo	Descrição
superposition_num	Não	Integer	O multiplicador máximo que você pode usar para quebras consecutivas. O número de avarias é contado a partir de 0 sempre que a duração da proteção contra avarias acumulada atinge 3.600s. Por exemplo, suponha que o Tempo de Inatividade Inicial (s) esteja definido como 180s e <b>Multiplier for Consecutive Breakdowns</b> esteja definido como 3. Se a avaria for acionada pela segunda vez, ou seja, menos de 3, a duração da proteção é de 360s (180s X 2). Se a avaria for acionada pelo terceiro ou quarto tempo, ou seja, igual ou superior a 3, a duração da proteção é de 540s (180s X 3). Quando a duração do tempo de inatividade acumulado excede 1 hora (3.600s), o número de avarias é contado a partir de 0.
suspend_num	Não	Integer	Limite do número de solicitações de URL pendentes. A proteção de conexão é acionada quando o limite é atingido.
sus_block_time	Não	Integer	Duração do tempo de inatividade após a proteção da conexão ser acionada. Durante esse período, o WAF deixa de encaminhar solicitações de sites.

**Tabela 4-48** TimeoutConfig

Parâmetro	Obrigatório	Tipo	Descrição
connect_timeout	Não	Integer	Tempo limite para o WAF se conectar ao servidor de origem.
send_timeout	Não	Integer	Tempo limite para o WAF enviar solicitações ao servidor de origem.
read_timeout	Não	Integer	Tempo limite para o WAF receber respostas do servidor de origem.

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-49** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio conectado a uma instância WAF na nuvem
policyid	String	ID da política
domainid	String	ID da conta.
projectid	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
enterprise_project_id	String	ID do projeto empresarial
protocol	String	Tipo de protocolo de back-end
server	Array of <b>CloudWafServer</b> objects	Configuração do servidor de origem do nome de domínio protegido
proxy	Boolean	Se um proxy é usado para o nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>false</b>: Nenhum proxy é usado.</li> <li>● <b>true</b>: Um proxy é usado.</li> </ul>
protect_status	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>
access_status	Integer	Status de acesso ao nome de domínio. O valor pode ser <b>0</b> ou <b>1</b> . <b>0</b> : O tráfego do site não foi encaminhado para o WAF. <b>1</b> : O tráfego do site foi encaminhado para o WAF.
access_code	String	Prefixo CNAME

Parâmetro	Tipo	Descrição
locked	Integer	Este parâmetro é reservado, que será usado para congelar um nome de domínio.
timestamp	Long	Hora em que o nome de domínio foi adicionado ao WAF.
certificateid	String	ID do certificado HTTPS.
certificatename	String	Nome do certificado
tls	String	Versão SSL Valores de enumeração: <ul style="list-style-type: none"> <li>● TLS v1.0</li> <li>● TLS v1.1</li> <li>● TLS v1.2</li> <li>● TLS v1.3</li> </ul>
cipher	String	Suíte Cipher. O valor pode ser <b>cipher_1</b> , <b>cipher_2</b> , <b>cipher_3</b> , <b>cipher_4</b> , ou <b>cipher_default</b> : <b>cipher_1</b> : ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH <b>cipher_2</b> : ECDH+AESGCM:EDH+AESGCM <b>cipher_3</b> : ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH <b>cipher_4</b> : ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH <b>cipher_default</b> : The cryptographic algorithms are ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM. Valores de enumeração: <ul style="list-style-type: none"> <li>● cipher_1</li> <li>● cipher_2</li> <li>● cipher_3</li> <li>● cipher_4</li> <li>● cipher_default</li> </ul>
block_page	<b>BlockPage</b> object	Configuração da página de alarme
extend	Map<String,String>	Identificador especial, que é usado no console.

Parâmetro	Tipo	Descrição
web_tag	String	Nome do site, que é o mesmo que o nome do site nos detalhes do nome de domínio no console do WAF.
traffic_mark	<b>TrafficMark</b> object	Identificador de tráfego
circuit_breaker	<b>CircuitBreaker</b> object	Configuração do disjuntor
lb_algorithm	String	Algoritmo de balanceamento de carga. O round robin ponderado é usado por padrão e não pode ser alterado. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>ip_hash</b></li> <li>● <b>round_robin</b></li> <li>● <b>session_hash</b></li> </ul>
timeout_config	<b>TimeoutConfig</b> object	Configurações de tempo limite
flag	<b>Flag</b> object	Identificador especial, que é usado no console.
description	String	Descrição do nome de domínio
http2_enable	Boolean	Suportar ou não HTTP/2. <ul style="list-style-type: none"> <li>● <b>true</b>: HTTP/2 é suportado.</li> <li>● <b>false</b>: HTTP/2 não é suportado.</li> </ul>
exclusive_ip	Boolean	Se usar um endereço IP dedicado. <ul style="list-style-type: none"> <li>● <b>true</b>: Use um endereço IP dedicado.</li> <li>● <b>false</b>: Não use um endereço IP dedicado.</li> </ul>
access_progress	Array of <b>Access_progress</b> objects	Progresso de acesso, que é usado apenas para o novo console (frontend).

**Tabela 4-50** CloudWafServer

Parâmetro	Tipo	Descrição
front_protocol	String	Protocolo usado pelo cliente para solicitar acesso ao servidor de origem. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>HTTP</b></li> <li>● <b>HTTPS</b></li> </ul>

Parâmetro	Tipo	Descrição
back_protocol	String	Protocolo usado pelo WAF para encaminhar solicitações de clientes recebidas aos servidores de origem Valores de enumeração: <ul style="list-style-type: none"> <li>● HTTP</li> <li>● HTTPS</li> </ul>
weight	Integer	Peso do servidor de origem. O algoritmo de balanceamento de carga encaminha solicitações para o servidor de origem com base no peso. O valor padrão é 1. Este campo não é incluído pelo WAF na nuvem.
address	String	Endereço IP do servidor de origem solicitado pelo cliente
port	Integer	Porta usada pelo WAF para encaminhar solicitações de clientes para o servidor de origem
type	String	Formato de endereço IP do servidor de origem, IPv4 e IPv6 Valores de enumeração: <ul style="list-style-type: none"> <li>● ipv4</li> <li>● ipv6</li> </ul>

**Tabela 4-51** BlockPage

Parâmetro	Tipo	Descrição
template	String	Nome do modelo
custom_page	<b>CustomPage</b> object	Página de alarme personalizada
redirect_url	String	URL da página redirecionada

**Tabela 4-52** CustomPage

Parâmetro	Tipo	Descrição
status_code	String	Códigos de status
content_type	String	O tipo de conteúdo da página de alarme personalizada. O valor pode ser <b>text/html</b> , <b>text/xml</b> , ou <b>application/json</b> .



Parâmetro	Tipo	Descrição
content	String	O conteúdo da página com base no tipo de página selecionado. Para obter detalhes, consulte o <i>Guia de usuário do Web Application Firewall (WAF)</i> .

**Tabela 4-53** TrafficMark

Parâmetro	Tipo	Descrição
sip	Array of strings	Etiqueta IP. Campo do cabeçalho da solicitação HTTP do endereço IP original do cliente.
cookie	String	Tag da sessão. Essa tag é usada por regras de origem de ataque conhecidas para bloquear ataques maliciosos com base em atributos de cookies. Esse parâmetro deve ser configurado em regras de origem de ataque conhecidas para bloquear solicitações com base em atributos de cookie.
params	String	Tag do usuário. Essa tag é usada por regras de origem de ataque conhecidas para bloquear ataques maliciosos com base em atributos de params. Esse parâmetro deve ser configurado para bloquear solicitações com base nos atributos params.

**Tabela 4-54** CircuitBreaker

Parâmetro	Tipo	Descrição
switch	Boolean	Se deve ativar a proteção de conexão. <ul style="list-style-type: none"> <li>● <b>true</b>: Ative a proteção de conexão.</li> <li>● <b>false</b>: Desative a proteção de conexão.</li> </ul>
dead_num	Integer	Limite de erro 502/504. 502/504 erros permitidos a cada 30 segundos.
dead_ratio	Number	Uma proteção contra avarias é acionada quando o limite de erro 502/504 e o limite percentual foram atingidos.
block_time	Integer	Período de proteção após a primeira quebra. Durante esse período, o WAF deixa de encaminhar solicitações de clientes.

Parâmetro	Tipo	Descrição
superposition_num	Integer	O multiplicador máximo que você pode usar para quebras consecutivas. O número de avarias é contado a partir de 0 sempre que a duração da proteção contra avarias acumulada atinge 3.600s. Por exemplo, suponha que o Tempo de Inatividade Inicial (s) esteja definido como 180s e <b>Multiplier for Consecutive Breakdowns</b> esteja definido como 3. Se a avaria for acionada pela segunda vez, ou seja, menos de 3, a duração da proteção é de 360s (180s X 2). Se a avaria for acionada pelo terceiro ou quarto tempo, ou seja, igual ou superior a 3, a duração da proteção é de 540s (180s X 3). Quando a duração do tempo de inatividade acumulado excede 1 hora (3.600s), o número de avarias é contado a partir de 0.
num_suspensão	número inteiro	Limite do número de solicitações de URL pendentes. A proteção de conexão é acionada quando o limite é atingido.
sus_block_time	número inteiro	Duração do tempo de inatividade após a proteção da conexão ser acionada. Durante esse período, o WAF deixa de encaminhar solicitações de sites.

**Tabela 4-55** TimeoutConfig

Parâmetro	Tipo	Descrição
connect_timeout	Integer	Tempo limite para o WAF se conectar ao servidor de origem.
send_timeout	Integer	Tempo limite para o WAF enviar solicitações ao servidor de origem.
read_timeout	Integer	Tempo limite para o WAF receber respostas do servidor de origem.

**Tabela 4-56** Bandeira

Parâmetro	Tipo	Descrição
pci_3ds	String	<p>Se o site passa a verificação de certificação PCI 3DS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI 3DS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação do PCI 3DS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
pci_dss	String	<p>Se o site passou na verificação de certificação PCI DSS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI DSS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação PCI DSS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cname	String	<p>O registro CNAME que está sendo usado.</p> <ul style="list-style-type: none"> <li>● <b>old</b>: O registro CNAME antigo é usado.</li> <li>● <b>new</b>: O novo registro CNAME é usado.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>old</b></li> <li>● <b>new</b></li> </ul>
is_dual_az	String	<p>Se o WAF suporta o Multi-AZ DR</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O WAF suporta DR multi-AZ.</li> <li>● <b>false</b>: O WAF não suporta DR multi-AZ.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ipv6	String	<p>Se a proteção IPv6 é suportada.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

**Tabela 4-57** Access\_progress

Parâmetro	Tipo	Descrição
step	Integer	Etapa
status	Integer	Estado. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: O passo não foi concluído.</li> <li>● <b>1</b>: O passo terminou.</li> </ul>

**Código de estado: 400**

**Tabela 4-58** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-59** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-60** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

{
  "server" : [ {
    "address" : "x.x.x.x",
    "port" : "80",
```

```
    "type" : "ipv4",
    "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
}
```

## Exemplo de respostas

**Código de estado: 200**

OK

```
{
  "id" : "e91ad96e379b4bea84f8fcda3d153370",
  "hostname" : "www.demo.com",
  "protocol" : "HTTP",
  "server" : [ {
    "address" : "x.x.x.x",
    "port" : 80,
    "type" : "ipv4",
    "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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.1.5 Exclusão de um nome de domínio do Cloud WAF

#### Função

Essa API é usada para excluir um nome de domínio do WAF da nuvem.

#### URI

DELETE /v1/{project\_id}/waf/instance/{instance\_id}

**Tabela 4-61** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
instance_id	Sim	String	ID do nome de domínio. Ele pode ser obtido chamando a API <b>ListHost</b> .

**Tabela 4-62** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-63** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-64** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostid	String	ID do nome de domínio
description	String	Descrição.
type	Integer	Modo de implantação do WAF. O valor predefinido é 1. Atualmente, apenas o proxy reverso é suportado.
proxy	Boolean	Se um proxy é usado para o nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>false</b>: Nenhum proxy é usado.</li> <li>● <b>true</b>: Um proxy é usado.</li> </ul>
flag	<b>Flag</b> object	Identificador especial, que é usado no console.
hostname	String	Nome de domínio adicionado ao WAF na nuvem.
access_code	String	Sufixo CNAME

Parâmetro	Tipo	Descrição
policyid	String	ID da política
timestamp	Long	Hora em que o nome de domínio foi adicionado ao WAF.
protect_status	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>
access_status	Integer	Status de acesso. <ul style="list-style-type: none"> <li>● <b>0</b>: O tráfego do site não foi encaminhado para o WAF. (Inacessível)</li> <li>● <b>1</b>: O tráfego do site foi encaminhado para o WAF. (Acessível)</li> </ul>
exclusive_ip	Boolean	Se usar um endereço IP dedicado. <ul style="list-style-type: none"> <li>● <b>true</b>: Use um endereço IP dedicado.</li> <li>● <b>false</b>: Não use um endereço IP dedicado.</li> </ul>
paid_type	String	Modo de pagamento baseado em pacote. Atualmente, apenas o modo pré-pago é suportado. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>prePaid</b></li> </ul>
web_tag	String	Nome do site

Tabela 4-65 Bandeira

Parâmetro	Tipo	Descrição
pci_3ds	String	Se o site passa a verificação de certificação PCI 3DS. <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI 3DS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação do PCI 3DS.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>



Parâmetro	Tipo	Descrição
pci_dss	String	Se o site passou na verificação de certificação PCI DSS. <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI DSS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação PCI DSS.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cname	String	O registro CNAME que está sendo usado. <ul style="list-style-type: none"> <li>● <b>old</b>: O registro CNAME antigo é usado.</li> <li>● <b>new</b>: O novo registro CNAME é usado.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>old</b></li> <li>● <b>new</b></li> </ul>
is_dual_az	String	Se o WAF suporta o Multi-AZ DR <ul style="list-style-type: none"> <li>● <b>true</b>: O WAF suporta DR multi-AZ.</li> <li>● <b>false</b>: O WAF não suporta DR multi-AZ.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ipv6	String	Se a proteção IPv6 é suportada. <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

**Código de estado: 400**

**Tabela 4-66** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-67** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-68** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.1.6 Alteração de status de proteção de um nome de domínio

#### Função

Alteração de status de proteção de um nome de domínio

#### URI

PUT /v1/{project\_id}/waf/instance/{instance\_id}/protect-status

**Tabela 4-69** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
instance_id	Sim	String	ID do nome de domínio. Este parâmetro é usado para especificar o nome de domínio cujo status de proteção você deseja modificar. Você pode obter o ID do nome de domínio chamando a API ( <b>ListHost</b> ) para consultar a lista de nomes de domínio protegidos com o WAF na nuvem.

**Tabela 4-70** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-71** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-72** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
protect_status	Sim	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-73** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
protect_status	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>

**Código de estado: 400**

**Tabela 4-74** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-75** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-76** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

Solicitação bem-sucedida.

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

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.1.7 Obtenção de informações de roteamento de nome de domínio (no modo nuvem)

### Função

Obtenção de informações de roteamento de nome de domínio (no modo nuvem)

### URI

GET /v1/{project\_id}/waf/instance/{instance\_id}/route

**Tabela 4-77** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
instance_id	Sim	String	ID do nome de domínio. Ele pode ser obtido chamando a API <b>ListHost</b> .

**Tabela 4-78** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-79** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

Código de estado: 200

**Tabela 4-80** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	Número de rotas
items	Array of <b>RouteBody</b> objects	Lista de rotas

**Tabela 4-81** RouteBody

Parâmetro	Tipo	Descrição
cname	String	Sufixo CNAME do cluster WAF
name	String	Nome do cluster do WAF
servers	Array of <b>RouteServerBody</b> objects	Lista de informações do servidor de origem do nome de domínio protegido

**Tabela 4-82** RouteServerBody

Parâmetro	Tipo	Descrição
back_protocol	String	Protocolo usado pelo WAF para encaminhar solicitações de clientes recebidas aos servidores de origem Valores de enumeração: <ul style="list-style-type: none"> <li>● HTTP</li> <li>● HTTPS</li> </ul>
address	String	Endereço IP do servidor de origem solicitado pelo cliente
port	Integer	Porta usada pelo WAF para encaminhar solicitações de clientes para o servidor de origem

**Código de estado: 400**

**Tabela 4-83** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro



**Código de estado: 401**

**Tabela 4-84** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-85** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Exemplos de solicitações**

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

**Exemplo de respostas**

**Código de estado: 200**

Solicitação bem-sucedida.

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

**Códigos de status**

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.

Código de status	Descrição
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.2 Gerenciamento de sites protegidos por mecanismos dedicados do WAF

### 4.2.1 Consulta de nomes de domínio protegidos por mecanismos WAF dedicados

#### Função

Essa API é usada para consultar a lista de nomes de domínio conectados a instâncias dedicadas do WAF.

#### URI

GET /v1/{project\_id}/premium-waf/host

**Tabela 4-86** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

**Tabela 4-87** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

Parâmetro	Obrigatório	Tipo	Descrição
page	Não	String	Número de página dos dados a serem retornados durante a consulta de paginação. Faixa de valor: <b>0</b> a <b>100.000</b> . O valor padrão é <b>1</b> , indicando que os dados na primeira página são retornados. Padrão: <b>1</b>
pagesize	Não	String	Número de resultados em cada página durante a consulta de paginação. Faixa de valor: <b>1</b> a <b>100</b> . O valor padrão é <b>10</b> , indicando que cada página contém 10 resultados. Padrão: <b>10</b>
hostname	Não	String	Nome de domínio
policyname	Não	String	Nome da política
protect_status	Não	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>

## Parâmetros de solicitação

**Tabela 4-88** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-89** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	Número total de nomes de domínio protegidos
items	Array of <b>SimplePremiumWafHost</b> objects	Matriz de detalhes sobre todos os nomes de domínio protegidos

**Tabela 4-90** SimplePremiumWafHost

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio
extend	Map<String,String>	Campo estendido, que é usado para salvar algumas informações de configuração sobre o nome de domínio protegido.
region	String	ID da região. Esse parâmetro é incluído quando o nome de domínio é adicionado ao WAF por meio do console. Esse parâmetro é deixado em branco quando o nome de domínio é adicionado ao WAF ao chamar uma API. Você pode consultar o ID da região na página Regiões e Endpoints no site da Huawei Cloud.
flag	<b>Flag</b> object	Identificador especial, que é usado no console.
description	String	Descrição do nome de domínio
policyid	String	ID da política usada inicialmente para o nome de domínio. Você pode chamar a API <b>ListPolicy</b> para consultar a lista de políticas e exibir o ID de uma política específica.

Parâmetro	Tipo	Descrição
protect_status	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>
access_status	Integer	Status de acesso ao nome de domínio. O valor pode ser <b>0</b> ou <b>1</b> . <b>0</b> : O tráfego do site não foi encaminhado para o WAF. <b>1</b> : O tráfego do site foi encaminhado para o WAF.
web_tag	String	Nome do site, que é o mesmo que o nome do site nos detalhes do nome de domínio no console do WAF.
hostid	String	ID de nome de domínio, que é o mesmo que o valor de id e é um campo redundante.

Tabela 4-91 Bandeira

Parâmetro	Tipo	Descrição
pci_3ds	String	Se o site passa a verificação de certificação PCI 3DS. <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI 3DS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação do PCI 3DS.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
pci_dss	String	Se o site passou na verificação de certificação PCI DSS. <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI DSS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação PCI DSS.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
cname	String	O registro CNAME que está sendo usado. <ul style="list-style-type: none"> <li>● <b>old</b>: O registro CNAME antigo é usado.</li> <li>● <b>new</b>: O novo registro CNAME é usado.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>old</b></li> <li>● <b>new</b></li> </ul>
is_dual_az	String	Se o WAF suporta o Multi-AZ DR <ul style="list-style-type: none"> <li>● <b>true</b>: O WAF suporta DR multi-AZ.</li> <li>● <b>false</b>: O WAF não suporta DR multi-AZ.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ipv6	String	Se a proteção IPv6 é suportada. <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

**Código de estado: 400**

**Tabela 4-92** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-93** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-94** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

```
GET https://{Endpoint}/v1/{project_id}/premium-waf/host?enterprise_project_id=0
```

## Exemplo de respostas

**Código de estado: 200**

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "ee896796e1a84f3f85865ae0853d8974",
    "hostname" : "www.demo.com",
    "extend" : { },
    "region" : "cn-north-4",
    "flag" : {
      "pci_3ds" : "false",
      "pci_dss" : "false"
    },
    "description" : "",
    "policyid" : "df15d0eb84194950a8fdc615b6c012dc",
    "protect_status" : 1,
    "access_status" : 0,
    "hostid" : "ee896796e1a84f3f85865ae0853d8974"
  } ]
}
```

## Códigos de status

Código de status	Descrição
200	OK
400	Pedido inválido
401	O token não tem a permissão necessária.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.2.2 Adição de um nome de domínio a uma instância dedicada do WAF

### Função

Essa API é usada para conectar um nome de domínio a uma instância dedicada do WAF.

### URI

POST /v1/{project\_id}/premium-waf/host

**Tabela 4-95** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

**Tabela 4-96** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

### Parâmetros de solicitação

**Tabela 4-97** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json; charset=utf8</b>
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).



**Tabela 4-98** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
certificateid	Não	String	ID do certificado. Ele pode ser obtido chamando a API <b>ListCertificates</b> . <ul style="list-style-type: none"> <li>● Este parâmetro não é necessário quando o protocolo do cliente é HTTP.</li> <li>● Este parâmetro é obrigatório quando o protocolo do cliente é HTTPS.</li> </ul>
certificatename	Não	String	Nome do certificado. <ul style="list-style-type: none"> <li>● Este parâmetro não é necessário quando o protocolo do cliente é HTTP.</li> <li>● Este parâmetro é obrigatório quando o protocolo do cliente é HTTPS.</li> </ul>
hostname	Sim	String	Nome de domínio protegido ou endereço IP (porta permitida)
proxy	Sim	Boolean	Se um proxy é usado para o nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>false</b>: Nenhum proxy é usado.</li> <li>● <b>true</b>: Um proxy é usado.</li> </ul>
policyid	Não	String	ID da política usada inicialmente para o nome de domínio. Você pode chamar a API <b>ListPolicy</b> para consultar a lista de políticas e exibir o ID de uma política específica.
server	Sim	Array of <b>PremiumWafServer</b> objects	Configuração do servidor de origem do nome de domínio protegido
block_page	Não	<b>BlockPage</b> object	Configuração da página de alarme. Este parâmetro é opcional. Quando uma página definida pelo usuário precisa ser configurada, todos os subcampos deste parâmetro são obrigatórios.
description	Não	String	Observações do nome de domínio protegido

**Tabela 4-99** PremiumWafServer

Parâmetro	Obrigatório	Tipo	Descrição
front_protocol	Sim	String	Protocolo usado pelo cliente para solicitar acesso ao servidor de origem. Valores de enumeração: ● <b>HTTP</b> ● <b>HTTPS</b>
back_protocol	Sim	String	Protocolo usado pelo WAF para encaminhar solicitações de clientes recebidas aos servidores de origem Valores de enumeração: ● <b>HTTP</b> ● <b>HTTPS</b>
weight	Não	Integer	Peso do servidor de origem. O algoritmo de balanceamento de carga encaminha solicitações para o servidor de origem com base no peso. O valor padrão é <b>1</b> . Este campo não é incluído pelo WAF na nuvem.
address	Sim	String	Endereço IP do servidor de origem solicitado pelo cliente
port	Sim	Integer	Porta usada pelo WAF para encaminhar solicitações de clientes para o servidor de origem
type	Sim	String	O endereço do servidor de origem é um endereço IPv4 ou IPv6. Valores de enumeração: ● <b>ipv4</b> ● <b>ipv6</b>

Parâmetro	Obrigatório	Tipo	Descrição
vpc_id	Sim	String	<p>ID de VPC. Para obter o ID da VPC, execute as seguintes etapas: Use um dos métodos a seguir para obter o ID da VPC.</p> <ul style="list-style-type: none"> <li>● Faça login no console do WAF e escolha <b>Instance Management &gt; Dedicated Engine &gt; VPC\Subnet</b>. O ID da VPC está na coluna <b>VPC \Subnet</b>.</li> <li>● Faça login no console da VPC e clique no nome da VPC. Na página exibida, copie o ID na área <b>VPC Information</b>.</li> </ul>

**Tabela 4-100** BlockPage

Parâmetro	Obrigatório	Tipo	Descrição
template	Sim	String	Nome do modelo
custom_page	Não	<b>CustomPage</b> object	Página de alarme personalizada
redirect_url	Não	String	URL da página redirecionada

**Tabela 4-101** CustomPage

Parâmetro	Obrigatório	Tipo	Descrição
status_code	Sim	String	Códigos de status
content_type	Sim	String	O tipo de conteúdo da página de alarme personalizada. O valor pode ser <b>text/html</b> , <b>text/xml</b> , ou <b>application/json</b> .
content	Sim	String	O conteúdo da página com base no tipo de página selecionado. Para obter detalhes, consulte o <i>Guia de usuário do Web Application Firewall (WAF)</i> .

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-102** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nomes de domínio protegidos
protocol	String	Protocolo do cliente. o protocolo usado por um cliente (por exemplo, um navegador) para acessar seu site. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>HTTPS</b></li> <li>● <b>HTTP</b></li> <li>● <b>HTTP&amp;HTTPS</b></li> </ul>
server	Array of <b>PremiumWafServer</b> objects	Configuração do servidor de origem do nome de domínio protegido
proxy	Boolean	Se deve usar um proxy <ul style="list-style-type: none"> <li>● <b>true</b>: Um proxy é usado.</li> <li>● <b>false</b>: Nenhum proxy é usado.</li> </ul>
locked	Integer	Status do nome de domínio. O valor pode ser <b>0</b> ou <b>1.0</b> : O nome de domínio não está congelado. <b>1</b> : O nome de domínio está congelado. Este parâmetro é redundante nesta versão.
timestamp	Long	Hora em que o nome de domínio foi adicionado ao WAF. O valor é um carimbo de data/hora de 13 dígitos em ms.
tls	String	Versão TLS. Você pode usar o TLS v1.0, TLS v1.1 ou TLS v1.2. O TLS v1.0 é usado por padrão. O parâmetro <b>tls</b> está disponível somente quando o protocolo do cliente é HTTPS. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>TLS v1.0</b></li> <li>● <b>TLS v1.1</b></li> <li>● <b>TLS v1.2</b></li> <li>● <b>TLS v1.3</b></li> </ul>

Parâmetro	Tipo	Descrição
cipher	String	<p>A <b>cipher</b> de parâmetro é necessária somente quando o protocolo do cliente é HTTPS. O valor pode ser <b>cipher_1</b>, <b>cipher_2</b>, <b>cipher_3</b>, <b>cipher_4</b>, ou <b>cipher_default</b>.</p> <ul style="list-style-type: none"> <li>● <b>cipher_1</b>: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH</li> <li>● <b>cipher_2</b>: ECDH+AESGCM:EDH+AESGCM</li> <li>● <b>cipher_3</b>: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH</li> <li>● <b>cipher_4</b>: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH</li> <li>● <b>cipher_default</b>: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>cipher_1</b></li> <li>● <b>cipher_2</b></li> <li>● <b>cipher_3</b></li> <li>● <b>cipher_4</b></li> <li>● <b>cipher_default</b></li> </ul>
extend	Map<String,String>	Campo estendido, que é usado para salvar algumas informações de configuração sobre o nome de domínio protegido.
flag	<b>Flag</b> object	Identificador especial, que é usado no console.
description	String	Descrição do nome de domínio
policyid	String	ID da política usada inicialmente para o nome de domínio. Você pode chamar a API <b>ListPolicy</b> para consultar a lista de políticas e exibir o ID de uma política específica.
domainid	String	ID da conta, que é o mesmo que o ID da conta na página <b>My Credentials</b> . Para acessar esta página, faça login no console de gerenciamento do Huawei Cloud, passe o cursor sobre seu nome de usuário e clique em <b>My Credentials</b> na janela exibida.

Parâmetro	Tipo	Descrição
projectid	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
enterprise_project_id	String	ID do projeto empresarial. Para obter a ID, faça login primeiro no console de gerenciamento do Huawei Cloud. Na barra de menus na parte superior da página, escolha <b>Enterprise &gt; Project Management</b> . Em seguida, clique no nome do projeto e visualize o ID.
protect_status	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>
access_status	Integer	Status de acesso ao nome de domínio. O valor pode ser <b>0</b> ou <b>1</b> . <b>0</b> : O tráfego do site não foi encaminhado para o WAF. <b>1</b> : O tráfego do site foi encaminhado para o WAF.
página_bloco	<b>BlockPage</b> object	Configuração da página de alarme

**Tabela 4-103** PremiumWafServer

Parâmetro	Tipo	Descrição
front_protocol	String	Protocolo usado pelo cliente para solicitar acesso ao servidor de origem. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>HTTP</b></li> <li>● <b>HTTPS</b></li> </ul>

Parâmetro	Tipo	Descrição
back_protocol	String	<p>Protocolo usado pelo WAF para encaminhar solicitações de clientes recebidas aos servidores de origem</p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>HTTP</b></li> <li>● <b>HTTPS</b></li> </ul>
weight	Integer	<p>Peso do servidor de origem. O algoritmo de balanceamento de carga encaminha solicitações para o servidor de origem com base no peso. O valor padrão é <b>1</b>. Este campo não é incluído pelo WAF na nuvem.</p>
address	String	<p>Endereço IP do servidor de origem solicitado pelo cliente</p>
port	Integer	<p>Porta usada pelo WAF para encaminhar solicitações de clientes para o servidor de origem</p>
type	String	<p>O endereço do servidor de origem é um endereço IPv4 ou IPv6.</p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>ipv4</b></li> <li>● <b>ipv6</b></li> </ul>
vpc_id	String	<p>ID de VPC. Para obter o ID da VPC, execute as seguintes etapas: Use um dos métodos a seguir para obter o ID da VPC.</p> <ul style="list-style-type: none"> <li>● Faça login no console do WAF e escolha <b>Instance Management &gt; Dedicated Engine &gt; VPC \Subnet</b>. O ID da VPC está na coluna <b>VPC \Subnet</b>.</li> <li>● Faça login no console da VPC e clique no nome da VPC. Na página exibida, copie o ID na área <b>VPC Information</b>.</li> </ul>

**Tabela 4-104** Bandeira

Parâmetro	Tipo	Descrição
pci_3ds	String	<p>Se o site passa a verificação de certificação PCI 3DS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI 3DS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação do PCI 3DS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
pci_dss	String	<p>Se o site passou na verificação de certificação PCI DSS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI DSS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação PCI DSS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cname	String	<p>O registro CNAME que está sendo usado.</p> <ul style="list-style-type: none"> <li>● <b>old</b>: O registro CNAME antigo é usado.</li> <li>● <b>new</b>: O novo registro CNAME é usado.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>old</b></li> <li>● <b>new</b></li> </ul>
is_dual_az	String	<p>Se o WAF suporta o Multi-AZ DR</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O WAF suporta DR multi-AZ.</li> <li>● <b>false</b>: O WAF não suporta DR multi-AZ.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ipv6	String	<p>Se a proteção IPv6 é suportada.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>



**Tabela 4-105** BlockPage

Parâmetro	Tipo	Descrição
template	String	Nome do modelo
custom_page	<b>CustomPage</b> object	Página de alarme personalizada
redirect_url	String	URL da página redirecionada

**Tabela 4-106** CustomPage

Parâmetro	Tipo	Descrição
status_code	String	Códigos de status
content_type	String	O tipo de conteúdo da página de alarme personalizada. O valor pode ser <b>text/html</b> , <b>text/xml</b> , ou <b>application/json</b> .
content	String	O conteúdo da página com base no tipo de página selecionado. Para obter detalhes, consulte o <i>Guia de usuário do Web Application Firewall (WAF)</i> .

**Código de estado: 400**

**Tabela 4-107** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-108** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-109** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

```
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" : ""
}
```

## Exemplo de respostas

**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 status

Código de status	Descrição
200	OK
400	Pedido inválido.
401	O token não tem a permissão necessária.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.2.3 Modificação de um nome de domínio protegido por uma instância WAF dedicada

#### Função

Essa API é usada para atualizar configurações de nomes de domínio protegidos com uma instância dedicada do WAF. As novas informações do servidor de origem substituirão as informações do servidor de origem antigo. Se você quiser manter as informações antigas, forneça-as como dados novos. Você pode fornecer apenas as informações atualizadas no corpo da solicitação.

#### URI

PUT /v1/{project\_id}/premium-waf/host/{host\_id}

Tabela 4-110 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
host_id	Sim	String	ID do nome de domínio protegido pelo mecanismo WAF dedicado

**Tabela 4-111** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-112** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).

**Tabela 4-113** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
proxy	Não	Boolean	Se um proxy é usado para o nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>false</b>: Nenhum proxy é usado.</li> <li>● <b>true</b>: Um proxy é usado.</li> </ul>
certificateid	Não	String	ID do certificado. Ele pode ser obtido chamando a API <b>ListCertificates</b> . <ul style="list-style-type: none"> <li>● Este parâmetro não é necessário quando o protocolo do cliente é HTTP.</li> <li>● Este parâmetro é obrigatório quando o protocolo do cliente é HTTPS.</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
certificatename	Não	String	Nome do certificado. <ul style="list-style-type: none"><li>● Este parâmetro não é necessário quando o protocolo do cliente é HTTP.</li><li>● Este parâmetro é obrigatório quando o protocolo do cliente é HTTPS.</li></ul>
tls	Não	String	Versão TLS. O TLS v1.0 é suportado por predefinição. Valores de enumeração: <ul style="list-style-type: none"><li>● <b>TLS v1.0</b></li><li>● <b>TLS v1.1</b></li><li>● <b>TLS v1.2</b></li><li>● <b>TLS v1.3</b></li></ul>

Parâmetro	Obrigatório	Tipo	Descrição
cipher	Não	String	<p>Suíte Cipher. O valor pode ser <b>cipher_1</b>, <b>cipher_2</b>, <b>cipher_3</b>, <b>cipher_4</b>, ou <b>cipher_default</b>:</p> <ul style="list-style-type: none"> <li>● <b>cipher_1</b>: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH</li> <li>● <b>cipher_2</b>: ECDH+AESGCM:EDH+AESGCM</li> <li>● <b>cipher_3</b>: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH</li> <li>● <b>cipher_4</b>: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH</li> <li>● <b>cipher_default</b>: The cryptographic algorithms are ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>cipher_1</b></li> <li>● <b>cipher_2</b></li> <li>● <b>cipher_3</b></li> <li>● <b>cipher_4</b></li> <li>● <b>cipher_default</b></li> </ul>
mode	Não	String	<p>Nó de nome de domínio especial no modo dedicado. Esse parâmetro é necessário apenas para modos WAF especiais, como ELB.</p>

Parâmetro	Obrigatório	Tipo	Descrição
locked	Não	Integer	Este parâmetro é reservado, que será usado para congelar um nome de domínio.
protect_status	Não	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>
access_status	Não	Integer	Status de acesso ao nome de domínio. O valor pode ser <b>0</b> ou <b>1</b> . <b>0</b> : O tráfego do site não foi encaminhado para o WAF. <b>1</b> : O tráfego do site foi encaminhado para o WAF.
timestamp	Não	Integer	Timestamp.
pool_ids	Não	Array of strings	Grupo de mecanismo dedicado ao qual o nome de domínio foi adicionado. Esse parâmetro é necessário somente no modo WAF especial, como o modo ELB.
block_page	Não	<b>BlockPage</b> object	Configuração da página de alarme
traffic_mark	Não	<b>TrafficMark</b> object	Identificador de tráfego
circuit_breaker	Não	<b>CircuitBreaker</b> object	Configuração do disjuntor
timeout_config	Não	<b>TimeoutConfig</b> object	Configurações de tempo limite

**Tabela 4-114** BlockPage

Parâmetro	Obrigatório	Tipo	Descrição
template	Sim	String	Nome do modelo
custom_page	Não	<b>CustomPage</b> object	Página de alarme personalizada
redirect_url	Não	String	URL da página redirecionada

**Tabela 4-115** CustomPage

Parâmetro	Obrigatório	Tipo	Descrição
status_code	Sim	String	Códigos de status
content_type	Sim	String	O tipo de conteúdo da página de alarme personalizada. O valor pode ser <b>text/html</b> , <b>text/xml</b> , ou <b>application/json</b> .
content	Sim	String	O conteúdo da página com base no tipo de página selecionado. Para obter detalhes, consulte o <i>Guia de usuário do Web Application Firewall (WAF)</i> .

**Tabela 4-116** TrafficMark

Parâmetro	Obrigatório	Tipo	Descrição
sip	Não	Array of strings	Etiqueta IP. Campo do cabeçalho da solicitação HTTP do endereço IP original do cliente.
cookie	Não	String	Tag da sessão. Essa tag é usada por regras de origem de ataque conhecidas para bloquear ataques maliciosos com base em atributos de cookies. Esse parâmetro deve ser configurado em regras de origem de ataque conhecidas para bloquear solicitações com base em atributos de cookie.



Parâmetro	Obrigatório	Tipo	Descrição
params	Não	String	Tag do usuário. Essa tag é usada por regras de origem de ataque conhecidas para bloquear ataques maliciosos com base em atributos de params. Esse parâmetro deve ser configurado para bloquear solicitações com base nos atributos params.

**Tabela 4-117** CircuitBreaker

Parâmetro	Obrigatório	Tipo	Descrição
switch	Não	Boolean	Se deve ativar a proteção de conexão. <ul style="list-style-type: none"> <li>● <b>true</b>: Ative a proteção de conexão.</li> <li>● <b>false</b>: Desative a proteção de conexão.</li> </ul>
dead_num	Não	Integer	Limite de erro 502/504. 502/504 erros permitidos a cada 30 segundos.
dead_ratio	Não	Number	Uma proteção contra avarias é acionada quando o limite de erro 502/504 e o limite percentual foram atingidos.
block_time	Não	Integer	Período de proteção após a primeira quebra. Durante esse período, o WAF deixa de encaminhar solicitações de clientes.

Parâmetro	Obrigatório	Tipo	Descrição
superposition_num	Não	Integer	O multiplicador máximo que você pode usar para quebras consecutivas. O número de avarias é contado a partir de 0 sempre que a duração da proteção contra avarias acumulada atinge 3.600s. Por exemplo, suponha que o Tempo de Inatividade Inicial (s) esteja definido como 180s e <b>Multiplier for Consecutive Breakdowns</b> esteja definido como 3. Se a avaria for acionada pela segunda vez, ou seja, menos de 3, a duração da proteção é de 360s (180s X 2). Se a avaria for acionada pelo terceiro ou quarto tempo, ou seja, igual ou superior a 3, a duração da proteção é de 540s (180s X 3). Quando a duração do tempo de inatividade acumulado excede 1 hora (3.600s), o número de avarias é contado a partir de 0.
suspend_num	Não	Integer	Limite do número de solicitações de URL pendentes. A proteção de conexão é acionada quando o limite é atingido.
sus_block_time	Não	Integer	Duração do tempo de inatividade após a proteção da conexão ser acionada. Durante esse período, o WAF deixa de encaminhar solicitações de sites.

**Tabela 4-118** TimeoutConfig

Parâmetro	Obrigatório	Tipo	Descrição
connect_timeout	Não	Integer	Tempo limite para o WAF se conectar ao servidor de origem.
send_timeout	Não	Integer	Tempo limite para o WAF enviar solicitações ao servidor de origem.
read_timeout	Não	Integer	Tempo limite para o WAF receber respostas do servidor de origem.

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-119** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio adicionado à instância dedicada do WAF
protocol	String	Protocolo do cliente. o protocolo usado por um cliente (por exemplo, um navegador) para acessar seu site.
server	Array of <b>PremiumWafServer</b> objects	Configuração do servidor de origem do nome de domínio protegido
proxy	Boolean	Se um proxy é usado para o nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>false</b>: Nenhum proxy é usado.</li> <li>● <b>true</b>: Um proxy é usado.</li> </ul>
locked	Integer	Este parâmetro é reservado, que será usado para congelar um nome de domínio. Padrão: <b>0</b>
timestamp	Long	Hora em que o nome de domínio foi adicionado ao WAF.
tls	String	Versão mínima do TLS. O valor pode ser <b>TLS v1.0</b> , <b>TLS v1.1</b> , ou <b>TLS v1.2</b> . O TLS v1.0 é usado por padrão. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>TLS v1.0</b></li> <li>● <b>TLS v1.1</b></li> <li>● <b>TLS v1.2</b></li> <li>● <b>TLS v1.3</b></li> </ul>

Parâmetro	Tipo	Descrição
cipher	String	<p>Suíte Cipher. O valor pode ser <b>cipher_1</b>, <b>cipher_2</b>, <b>cipher_3</b>, <b>cipher_4</b>, ou <b>cipher_default</b>: <b>cipher_1</b>: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH</p> <ul style="list-style-type: none"> <li>● <b>cipher_2</b>: ECDH+AESGCM:EDH+AESGCM</li> <li>● <b>cipher_3</b>: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH</li> <li>● <b>cipher_4</b>: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH</li> <li>● <b>cipher_default</b>: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>cipher_1</b></li> <li>● <b>cipher_2</b></li> <li>● <b>cipher_3</b></li> <li>● <b>cipher_4</b></li> <li>● <b>cipher_default</b></li> </ul>
extend	Map<String,String>	Campo estendido, que é usado para salvar algumas informações de configuração sobre o nome de domínio protegido.
flag	<b>Flag</b> object	Identificador especial, que é usado no console.
description	String	Descrição do nome de domínio
policyid	String	ID da política usada inicialmente para o nome de domínio. Você pode chamar a API <b>ListPolicy</b> para consultar a lista de políticas e exibir o ID da política específica.
domainid	String	ID da conta, que é o mesmo que o ID da conta na página <b>My Credentials</b> . Para acessar esta página, faça login no console de gerenciamento do Huawei Cloud, passe o cursor sobre seu nome de usuário e clique em <b>My Credentials</b> na janela exibida.

Parâmetro	Tipo	Descrição
projectid	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
enterprise_project_id	String	ID do projeto empresarial. Para obter a ID, faça login primeiro no console de gerenciamento do Huawei Cloud. Na barra de menus na parte superior da página, escolha <b>Enterprise &gt; Project Management</b> . Em seguida, clique no nome do projeto e visualize o ID.
certificateid	String	ID do certificado HTTPS.
certificatename	String	Nome do certificado
protect_status	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>
access_status	Integer	Status de acesso ao nome de domínio. O valor pode ser <b>0</b> ou <b>1</b> . <b>0</b> : O tráfego do site não foi encaminhado para o WAF. <b>1</b> : O tráfego do site foi encaminhado para o WAF.
web_tag	String	Nome do site, que é o mesmo que o nome do site nos detalhes do nome de domínio no console do WAF.
lb_algorithm	String	Algoritmo de balanceamento de carga. O round robin ponderado é usado por padrão e não pode ser alterado.
block_page	<b>BlockPage</b> object	Configuração da página de alarme
traffic_mark	<b>TrafficMark</b> object	Identificador de tráfego
timeout_config	<b>TimeoutConfig</b> object	Configurações de tempo limite
access_progress	Array of <b>AccessProgress</b> objects	Progresso do acesso, que é usado apenas para o novo console do WAF.

**Tabela 4-120** PremiumWafServer

Parâmetro	Tipo	Descrição
front_protocol	String	Protocolo usado pelo cliente para solicitar acesso ao servidor de origem. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>HTTP</b></li> <li>● <b>HTTPS</b></li> </ul>
back_protocol	String	Protocolo usado pelo WAF para encaminhar solicitações de clientes recebidas aos servidores de origem Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>HTTP</b></li> <li>● <b>HTTPS</b></li> </ul>
weight	Integer	Peso do servidor de origem. O algoritmo de balanceamento de carga encaminha solicitações para o servidor de origem com base no peso. O valor padrão é 1. Este campo não é incluído pelo WAF na nuvem.
address	String	Endereço IP do servidor de origem solicitado pelo cliente
port	Integer	Porta usada pelo WAF para encaminhar solicitações de clientes para o servidor de origem
type	String	O endereço do servidor de origem é um endereço IPv4 ou IPv6. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>ipv4</b></li> <li>● <b>ipv6</b></li> </ul>
vpc_id	String	ID de VPC Para obter o ID da VPC, execute as seguintes etapas: Use um dos métodos a seguir para obter o ID da VPC. <ul style="list-style-type: none"> <li>● Faça login no console do WAF e escolha <b>Instance Management &gt; Dedicated Engine &gt; VPC \Subnet</b>. O ID da VPC está na coluna <b>VPC \Subnet</b>.</li> <li>● Faça login no console da VPC e clique no nome da VPC. Na página exibida, copie o ID na área <b>VPC Information</b>.</li> </ul>

**Tabela 4-121** Bandeira

Parâmetro	Tipo	Descrição
pci_3ds	String	<p>Se o site passa a verificação de certificação PCI 3DS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI 3DS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação do PCI 3DS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
pci_dss	String	<p>Se o site passou na verificação de certificação PCI DSS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI DSS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação PCI DSS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cname	String	<p>O registro CNAME que está sendo usado.</p> <ul style="list-style-type: none"> <li>● <b>old</b>: O registro CNAME antigo é usado.</li> <li>● <b>new</b>: O novo registro CNAME é usado.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>old</b></li> <li>● <b>new</b></li> </ul>
is_dual_az	String	<p>Se o WAF suporta o Multi-AZ DR</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O WAF suporta DR multi-AZ.</li> <li>● <b>false</b>: O WAF não suporta DR multi-AZ.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ipv6	String	<p>Se a proteção IPv6 é suportada.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

**Tabela 4-122** BlockPage

Parâmetro	Tipo	Descrição
template	String	Nome do modelo
custom_page	<b>CustomPage</b> object	Página de alarme personalizada
redirect_url	String	URL da página redirecionada

**Tabela 4-123** CustomPage

Parâmetro	Tipo	Descrição
status_code	String	Códigos de status
content_type	String	O tipo de conteúdo da página de alarme personalizada. O valor pode ser <b>text/html</b> , <b>text/xml</b> , ou <b>application/json</b> .
content	String	O conteúdo da página com base no tipo de página selecionado. Para obter detalhes, consulte o <i>Guia de usuário do Web Application Firewall (WAF)</i> .

**Tabela 4-124** TrafficMark

Parâmetro	Tipo	Descrição
sip	Array of strings	Etiqueta IP. Campo do cabeçalho da solicitação HTTP do endereço IP original do cliente.
cookie	String	Tag da sessão. Essa tag é usada por regras de origem de ataque conhecidas para bloquear ataques maliciosos com base em atributos de cookies. Esse parâmetro deve ser configurado em regras de origem de ataque conhecidas para bloquear solicitações com base em atributos de cookie.
params	String	Tag do usuário. Essa tag é usada por regras de origem de ataque conhecidas para bloquear ataques maliciosos com base em atributos de params. Esse parâmetro deve ser configurado para bloquear solicitações com base nos atributos params.



**Tabela 4-125** TimeoutConfig

Parâmetro	Tipo	Descrição
connect_timeout	Integer	Tempo limite para o WAF se conectar ao servidor de origem.
send_timeout	Integer	Tempo limite para o WAF enviar solicitações ao servidor de origem.
read_timeout	Integer	Tempo limite para o WAF receber respostas do servidor de origem.

**Tabela 4-126** Access\_progress

Parâmetro	Tipo	Descrição
step	Integer	Etapa
status	Integer	Estado. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: O passo não foi concluído.</li> <li>● <b>1</b>: O passo terminou.</li> </ul>

**Código de estado: 400**

**Tabela 4-127** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-128** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-129** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

```
{
  "proxy" : "false\r"
}
```

## Exemplo de respostas

**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 status

Código de status	Descrição
200	OK
400	Pedido inválido.
401	O token não tem a permissão necessária.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.2.4 Consulta de configurações de nome de domínio no modo dedicado

### Função

Essa API é usada para consultar configurações de nomes de domínio protegidos com instâncias WAF dedicadas.

### URI

GET /v1/{project\_id}/premium-waf/host/{host\_id}

**Tabela 4-130** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
host_id	Sim	String	ID do nome de domínio protegido pelo mecanismo WAF dedicado

**Tabela 4-131** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-132** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-133** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio adicionado à instância dedicada do WAF
protocol	String	Protocolo do cliente. o protocolo usado por um cliente (por exemplo, um navegador) para acessar seu site.
server	Array of <b>PremiumWafServer</b> objects	Configuração do servidor de origem do nome de domínio protegido
proxy	Boolean	Se um proxy é usado para o nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>false</b>: Nenhum proxy é usado.</li> <li>● <b>true</b>: Um proxy é usado.</li> </ul>
locked	Integer	Este parâmetro é reservado, que será usado para congelar um nome de domínio. Padrão: <b>0</b>
timestamp	Long	Hora em que o nome de domínio foi adicionado ao WAF.

Parâmetro	Tipo	Descrição
tls	String	<p>Versão mínima do TLS. Você pode usar o TLS v1.0, TLS v1.1 ou TLS v1.2. O TLS v1.0 é usado por padrão. O parâmetro <b>tls</b> é exigido somente quando o protocolo do cliente é HTTPS.</p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>TLS v1.0</b></li> <li>● <b>TLS v1.1</b></li> <li>● <b>TLS v1.2</b></li> <li>● <b>TLS v1.3</b></li> </ul>
cipher	String	<p>A <b>cipher</b> de parâmetro é necessária somente quando o protocolo do cliente é HTTPS. O valor pode ser <b>cipher_1</b>, <b>cipher_2</b>, <b>cipher_3</b>, <b>cipher_4</b>, ou <b>cipher_default</b>.</p> <ul style="list-style-type: none"> <li>● <b>cipher_1</b>: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH</li> <li>● <b>cipher_2</b>: ECDH+AESGCM:EDH+AESGCM</li> <li>● <b>cipher_3</b>: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH</li> <li>● <b>cipher_4</b>: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH</li> <li>● <b>cipher_default</b>: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>cipher_1</b></li> <li>● <b>cipher_2</b></li> <li>● <b>cipher_3</b></li> <li>● <b>cipher_4</b></li> <li>● <b>cipher_default</b></li> </ul>
extend	Map<String,String>	Campo estendido, que é usado para salvar algumas informações de configuração sobre o nome de domínio protegido.
flag	<b>Flag</b> object	Identificador especial, que é usado no console.
description	String	Descrição do nome de domínio

Parâmetro	Tipo	Descrição
policyid	String	ID da política usada inicialmente para o nome de domínio. Você pode chamar a API <b>ListPolicy</b> para consultar a lista de políticas e exibir o ID da política específica.
domainid	String	ID da conta, que é o mesmo que o ID da conta na página <b>My Credentials</b> . Para acessar esta página, faça login no console de gerenciamento do Huawei Cloud, passe o cursor sobre seu nome de usuário e clique em <b>My Credentials</b> na janela exibida.
projectid	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
enterprise_project_id	String	ID do projeto empresarial. Para obter a ID, faça login primeiro no console de gerenciamento do Huawei Cloud. Na barra de menus na parte superior da página, escolha <b>Enterprise &gt; Project Management</b> . Em seguida, clique no nome do projeto e visualize o ID.
certificateid	String	ID do certificado HTTPS.
certificatename	String	Nome do certificado
protect_status	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>
access_status	Integer	Status de acesso ao nome de domínio. O valor pode ser <b>0</b> ou <b>1</b> . <b>0</b> : O tráfego do site não foi encaminhado para o WAF. <b>1</b> : O tráfego do site foi encaminhado para o WAF.
web_tag	String	Nome do site, que é o mesmo que o nome do site nos detalhes do nome de domínio no console do WAF.
block_page	<b>BlockPage</b> object	Configuração da página de alarme
traffic_mark	<b>TrafficMark</b> object	Identificador de tráfego

Parâmetro	Tipo	Descrição
timeout_config	<b>TimeoutConfig</b> object	Configurações de tempo limite
access_progress	Array of <b>Access_progress</b> objects	Progresso do acesso, que é usado apenas para o novo console do WAF.

**Tabela 4-134** PremiumWafServer

Parâmetro	Tipo	Descrição
front_protocol	String	Protocolo usado pelo cliente para solicitar acesso ao servidor de origem. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>HTTP</b></li> <li>● <b>HTTPS</b></li> </ul>
back_protocol	String	Protocolo usado pelo WAF para encaminhar solicitações de clientes recebidas aos servidores de origem Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>HTTP</b></li> <li>● <b>HTTPS</b></li> </ul>
weight	Integer	Peso do servidor de origem. O algoritmo de balanceamento de carga encaminha solicitações para o servidor de origem com base no peso. O valor padrão é 1. Este campo não é incluído pelo WAF na nuvem.
address	String	Endereço IP do servidor de origem solicitado pelo cliente
port	Integer	Porta usada pelo WAF para encaminhar solicitações de clientes para o servidor de origem
type	String	O endereço do servidor de origem é um endereço IPv4 ou IPv6. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>ipv4</b></li> <li>● <b>ipv6</b></li> </ul>

Parâmetro	Tipo	Descrição
vpc_id	String	<p>ID de VPC Para obter o ID da VPC, execute as seguintes etapas: Use um dos métodos a seguir para obter o ID da VPC.</p> <ul style="list-style-type: none"> <li>● Faça login no console do WAF e escolha <b>Instance Management &gt; Dedicated Engine &gt; VPC \Subnet</b>. O ID da VPC está na coluna <b>VPC \Subnet</b>.</li> <li>● Faça login no console da VPC e clique no nome da VPC. Na página exibida, copie o ID na área <b>VPC Information</b>.</li> </ul>

Tabela 4-135 Bandeira

Parâmetro	Tipo	Descrição
pci_3ds	String	<p>Se o site passa a verificação de certificação PCI 3DS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI 3DS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação do PCI 3DS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
pci_dss	String	<p>Se o site passou na verificação de certificação PCI DSS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI DSS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação PCI DSS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cname	String	<p>O registro CNAME que está sendo usado.</p> <ul style="list-style-type: none"> <li>● <b>old</b>: O registro CNAME antigo é usado.</li> <li>● <b>new</b>: O novo registro CNAME é usado.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>old</b></li> <li>● <b>new</b></li> </ul>



Parâmetro	Tipo	Descrição
is_dual_az	String	Se o WAF suporta o Multi-AZ DR <ul style="list-style-type: none"> <li>● <b>true</b>: O WAF suporta DR multi-AZ.</li> <li>● <b>false</b>: O WAF não suporta DR multi-AZ.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ipv6	String	Se a proteção IPv6 é suportada. <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

**Tabela 4-136** BlockPage

Parâmetro	Tipo	Descrição
template	String	Nome do modelo
custom_page	<b>CustomPage</b> object	Página de alarme personalizada
redirect_url	String	URL da página redirecionada

**Tabela 4-137** CustomPage

Parâmetro	Tipo	Descrição
status_code	String	Códigos de status
content_type	String	O tipo de conteúdo da página de alarme personalizada. O valor pode ser <b>text/html</b> , <b>text/xml</b> , ou <b>application/json</b> .
content	String	O conteúdo da página com base no tipo de página selecionado. Para obter detalhes, consulte o <i>Guia de usuário do Web Application Firewall (WAF)</i> .

**Tabela 4-138** TrafficMark

Parâmetro	Tipo	Descrição
sip	Array of strings	Etiqueta IP. Campo do cabeçalho da solicitação HTTP do endereço IP original do cliente.
cookie	String	Tag da sessão. Essa tag é usada por regras de origem de ataque conhecidas para bloquear ataques maliciosos com base em atributos de cookies. Esse parâmetro deve ser configurado em regras de origem de ataque conhecidas para bloquear solicitações com base em atributos de cookie.
params	String	Tag do usuário. Essa tag é usada por regras de origem de ataque conhecidas para bloquear ataques maliciosos com base em atributos de params. Esse parâmetro deve ser configurado para bloquear solicitações com base nos atributos params.

**Tabela 4-139** TimeoutConfig

Parâmetro	Tipo	Descrição
connect_timeout	Integer	Tempo limite para o WAF se conectar ao servidor de origem.
send_timeout	Integer	Tempo limite para o WAF enviar solicitações ao servidor de origem.
read_timeout	Integer	Tempo limite para o WAF receber respostas do servidor de origem.

**Tabela 4-140** Access\_progress

Parâmetro	Tipo	Descrição
step	Integer	Etapa
status	Integer	Estado. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: O passo não foi concluído.</li> <li>● <b>1</b>: O passo terminou.</li> </ul>

**Código de estado: 400**

**Tabela 4-141** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-142** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-143** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

```
GET https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}?  
enterprise_project_id=0
```

## Exemplo de respostas

**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 status

Código de status	Descrição
200	OK
400	Pedido inválido
401	O token não tem a permissão necessária.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.2.5 Exclusão de um nome de domínio de uma instância dedicada do WAF

### Função

Essa API é usada para excluir um nome de domínio protegido com uma instância WAF dedicada.

### URI

DELETE /v1/{project\_id}/premium-waf/host/{host\_id}

**Tabela 4-144** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
host_id	Sim	String	ID do nome de domínio protegido pelo mecanismo WAF dedicado

**Tabela 4-145** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.
keepPolicy	Não	Boolean	Se a manter a regra. <b>false</b> : A política para o nome de domínio não será mantida. <b>true</b> : A política para o nome de domínio será mantida. Se a política usada para o nome de domínio que você deseja excluir também for usada para outros nomes de domínio, esse parâmetro deve ser deixado em branco. Padrão: 1

## Parâmetros de solicitação

**Tabela 4-146** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).

## Parâmetros de resposta

Código de estado: 200

Tabela 4-147 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio
extend	Map<String,String>	Campo estendido, que é usado para salvar algumas informações de configuração sobre o nome de domínio protegido.
region	String	ID da região. Esse parâmetro é incluído quando o nome de domínio é adicionado ao WAF por meio do console. Esse parâmetro é deixado em branco quando o nome de domínio é adicionado ao WAF ao chamar uma API. Você pode consultar o ID da região na página Regiões e Endpoints no site da Huawei Cloud.
flag	Flag object	Identificador especial, que é usado no console.
description	String	Descrição do nome de domínio
policyid	String	ID da política usada inicialmente para o nome de domínio. Você pode chamar a API <b>ListPolicy</b> para consultar a lista de políticas e exibir o ID de uma política específica.
protect_status	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"><li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li><li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li><li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li></ul>
access_status	Integer	Status de acesso ao nome de domínio. O valor pode ser <b>0</b> ou <b>1</b> . <b>0</b> : O tráfego do site não foi encaminhado para o WAF. <b>1</b> : O tráfego do site foi encaminhado para o WAF.
web_tag	String	Nome do site, que é o mesmo que o nome do site nos detalhes do nome de domínio no console do WAF.

Parâmetro	Tipo	Descrição
host_id	String	ID do nome de domínio, que é o mesmo que o valor de <i>*id</i> . Este campo é redundante.

Tabela 4-148 Bandeira

Parâmetro	Tipo	Descrição
pci_3ds	String	Se o site passa a verificação de certificação PCI 3DS. <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI 3DS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação do PCI 3DS.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
pci_dss	String	Se o site passou na verificação de certificação PCI DSS. <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI DSS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação PCI DSS.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cname	String	O registro CNAME que está sendo usado. <ul style="list-style-type: none"> <li>● <b>old</b>: O registro CNAME antigo é usado.</li> <li>● <b>new</b>: O novo registro CNAME é usado.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>old</b></li> <li>● <b>new</b></li> </ul>
is_dual_az	String	Se o WAF suporta o Multi-AZ DR <ul style="list-style-type: none"> <li>● <b>true</b>: O WAF suporta DR multi-AZ.</li> <li>● <b>false</b>: O WAF não suporta DR multi-AZ.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
ipv6	String	Se a proteção IPv6 é suportada. <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

**Código de estado: 400**

**Tabela 4-149** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-150** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-151** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

```
DELETE https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}?
enterprise_project_id=0
```



## Exemplo de respostas

**Código de estado: 200**

OK

```
{
  "id" : "ee896796e1a84f3f85865ae0853d8974",
  "hostname" : "www.demo.com",
  "region" : "cn-north-4",
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false"
  },
  "description" : "",
  "policyid" : "df15d0eb84194950a8fdc615b6c012dc",
  "protect_status" : 1,
  "access_status" : 0,
  "hostid" : "ee896796e1a84f3f85865ae0853d8974"
}
```

## Códigos de status

Código de status	Descrição
200	OK
400	Pedido inválido
401	O token não tem a permissão necessária.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.2.6 Modificação de status de proteção de um nome de domínio no modo dedicado

### Função

Essa API é usada para modificar o status de proteção de um nome de domínio conectado a uma instância dedicada do WAF.

### URI

PUT /v1/{project\_id}/premium-waf/host/{host\_id}/protect-status

**Tabela 4-152** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
host_id	Sim	String	ID do nome de domínio protegido pelo mecanismo WAF dedicado

**Tabela 4-153** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-154** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).

**Tabela 4-155** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
protect_status	Sim	Integer	<p>Status do WAF do nome de domínio protegido.</p> <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-156** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
protect_status	Integer	<p>Status do WAF do nome de domínio protegido.</p> <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>

**Código de estado: 400**

**Tabela 4-157** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro

Parâmetro	Tipo	Descrição
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-158** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-159** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

```
PUT https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}/protect-status?
enterprise_project_id=0

{
  "protect_status" : 1
}
```

## Exemplo de respostas

**Código de estado: 200**

OK

```
{
  "protect_status" : 1
}
```

## Códigos de status

Código de status	Descrição
200	OK
400	Pedido inválido

Código de status	Descrição
401	O token não tem a permissão necessária.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.3 Gerenciamento de políticas

### 4.3.1 Consulta de lista de políticas de proteção

#### Função

Essa API é usada para consultar a lista de políticas de proteção.

#### URI

GET /v1/{project\_id}/waf/policy

**Tabela 4-160** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

**Tabela 4-161** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

Parâmetro	Obrigatório	Tipo	Descrição
page	Não	Integer	Número de página dos dados a serem retornados durante a consulta de paginação. O valor padrão é <b>1</b> , indicando que os dados na primeira página são retornados. Padrão: <b>1</b>
pagesize	Não	Integer	Número de resultados em cada página durante a consulta de paginação. Faixa de valor: <b>1 a 100</b> . O valor padrão é <b>10</b> , indicando que cada página contém 10 resultados. Padrão: <b>10</b>
name	Não	String	Nome da política

## Parâmetros de solicitação

Tabela 4-162 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

Código de estado: **200**

Tabela 4-163 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	Número total de políticas
items	Array of <b>PolicyResponse</b> objects	Matriz de informações da política de proteção

**Tabela 4-164** PolicyResponse

Parâmetro	Tipo	Descrição
id	String	ID da política
name	String	Matriz de detalhes das políticas
level	Integer	<p>Nível de proteção da proteção básica da Web</p> <ul style="list-style-type: none"> <li>● <b>1</b>: Baixo. Nesse nível de proteção, o WAF bloqueia apenas solicitações com recursos óbvios de ataque. Se um grande número de alarmes falsos tiver sido relatado, recomenda-se <b>Low</b>.</li> <li>● <b>2</b>: Médio. Esse nível de proteção atende aos requisitos de proteção da Web na maioria dos cenários.</li> <li>● <b>3</b>: Alto. Nesse nível de proteção, o WAF fornece a melhor proteção granular e pode interceptar ataques com recursos complexos de desvio, como ataques cibernéticos Jolokia, detecção de vulnerabilidades de interface de gateway comum (CGI) e ataques de injeção Druid SQL.</li> </ul> <p>Padrão: <b>2</b></p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>1</b></li> <li>● <b>2</b></li> <li>● <b>3</b></li> </ul>
full_detection	Boolean	<p>O modo de detecção em Proteção Precisa.</p> <ul style="list-style-type: none"> <li>● <b>false</b>: Detecção instantânea. Quando uma solicitação atinge as condições de bloqueio na Proteção precisa, o WAF encerra as verificações e bloqueia a solicitação imediatamente.</li> <li>● <b>true</b>: Detecção completa. Se uma solicitação atingir as condições de bloqueio em Proteção precisa, o WAF não bloqueará a solicitação imediatamente. Em vez disso, ele bloqueia as solicitações até que outras verificações sejam concluídas.</li> </ul>
robot_action	<b>Action</b> object	Ações de proteção para cada regra na proteção anti-crawler.
action	<b>PolicyAction</b> object	Ação Protetora
options	<b>PolicyOption</b> object	Se um tipo de proteção está ativado na política de proteção.
modulex_options	Map<String, Object>	Configurações sobre controle de acesso inteligente. Atualmente, esse recurso ainda está na fase de teste beta aberto (OBT) e disponível em alguns sites.

Parâmetro	Tipo	Descrição
hosts	Array of strings	Matriz dos ID de nome de domínio protegidas pela política.
bind_host	Array of <b>BindHost</b> objects	Matriz de nomes de domínio protegidos com a política de proteção. Comparado com o campo <b>hosts</b> , este campo contém mais detalhes.
extend	Map<String,String>	Campo estendido, que é usado para armazenar a configuração de regras da proteção básica da Web.
timestamp	Long	Hora em que uma política é criada

Tabela 4-165 Ação

Parâmetro	Tipo	Descrição
category	String	Ação de proteção para regras anti-crawler baseadas em recursos: <ul style="list-style-type: none"> <li>● <b>log</b>: O WAF registra apenas os ataques descobertos.</li> <li>● <b>block</b>: WAF bloqueia ataques descobertos.</li> </ul>

Tabela 4-166 PolicyAction

Parâmetro	Tipo	Descrição
category	String	Ação básica de proteção da web. O valor pode ser <b>log</b> ou <b>block</b> . <b>log</b> : WAF apenas registra ataques descobertos. <b>block</b> : WAF bloqueia ataques descobertos. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>block</b></li> <li>● <b>log</b></li> </ul>

Tabela 4-167 PolicyOption

Parâmetro	Tipo	Descrição
webattack	Boolean	Se a proteção básica da Web está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>



Parâmetro	Tipo	Descrição
common	Boolean	Se a verificação geral está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler	Boolean	Este parâmetro é reservado. O valor deste parâmetro é fixado em <b>true</b> . Você pode ignorar esse parâmetro. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_engine	Boolean	Se o motor de busca está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_scanner	Boolean	Se a detecção anti-crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_script	Boolean	Se o JavaScript anti-crawler está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_other	Boolean	Se outra verificação de crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
webshell	Boolean	Se a detecção de webshell está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cc	Boolean	Se as regras de proteção contra ataques da CC estão ativadas Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
custom	Boolean	Se a proteção precisa está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
whiteblackip	Boolean	Se a proteção de lista negra e lista branca está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
geoip	Boolean	Se o controle de acesso de geolocalização está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ignore	Boolean	Se o mascaramento de alarme falso está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
privacy	Boolean	Se o mascaramento de dados está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
antitamper	Boolean	Se a proteção contra adulteração da Web está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
antileakage	Boolean	Se a prevenção de vazamento de informações está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
bot_enable	Boolean	Se a proteção anti-crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
modulex_enabled	Boolean	Se a proteção contra ataques CC para moduleX está ativada. Esse recurso está no teste beta aberto (OBT). Durante o OBT, somente o modo de registro somente é suportado. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

**Tabela 4-168** BindHost

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio
waf_type	String	Modo de implantação da instância do WAF usado para o nome de domínio. O valor pode ser <b>cloud</b> para WAF na nuvem ou <b>premium</b> para instâncias dedicadas do WAF.
mode	String	Este parâmetro é requerido apenas pelo modo dedicado.

**Código de estado: 400**

**Tabela 4-169** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-170** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-171** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

### Código de estado: 200

Solicitação bem-sucedida.

```
{
  "total" : 1,
  "items" : [ {
    "id" : "41cba8aee2e94bcdbf57460874205494",
    "name" : "policy_2FHwFOKz",
    "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,
      "whiteblackip" : true,
      "geoip" : true,
      "ignore" : true,
      "privacy" : true,
      "antitamper" : true,
      "antileakage" : false,
      "bot_enable" : true,
      "modulex_enabled" : false
    },
    "hosts" : [ ],
    "extend" : { },
    "timestamp" : 1650527546218,
    "full_detection" : false,
    "bind_host" : [ ]
  } ]
}
```

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.

Código de status	Descrição
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.3.2 Criação de uma política de proteção

#### Função

Essa API é usada para criar uma política de proteção. O sistema configura alguns itens de configuração padrão ao gerar a política. Para modificar os itens de configuração padrão, chame a API para atualizar a política de proteção.

#### URI

POST /v1/{project\_id}/waf/policy

Tabela 4-172 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

Tabela 4-173 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-174** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-175** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
name	Sim	String	Matriz de detalhes das políticas

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-176** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da política
name	String	Matriz de detalhes das políticas

Parâmetro	Tipo	Descrição
level	Integer	<p>Nível de proteção da proteção básica da Web</p> <ul style="list-style-type: none"> <li>● <b>1</b>: Baixo. Nesse nível de proteção, o WAF bloqueia apenas solicitações com recursos óbvios de ataque. Se um grande número de alarmes falsos tiver sido relatado, recomenda-se <b>Low</b>.</li> <li>● <b>2</b>: Médio. Esse nível de proteção atende aos requisitos de proteção da Web na maioria dos cenários.</li> <li>● <b>3</b>: Alto. Nesse nível de proteção, o WAF fornece a melhor proteção granular e pode interceptar ataques com recursos complexos de desvio, como ataques cibernéticos Jolokia, detecção de vulnerabilidades de interface de gateway comum (CGI) e ataques de injeção Druid SQL.</li> </ul> <p>Padrão: <b>2</b></p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>1</b></li> <li>● <b>2</b></li> <li>● <b>3</b></li> </ul>
full_detection	Boolean	<p>O modo de detecção em Proteção Precisa.</p> <ul style="list-style-type: none"> <li>● <b>false</b>: Detecção instantânea. Quando uma solicitação atinge as condições de bloqueio na Proteção precisa, o WAF encerra as verificações e bloqueia a solicitação imediatamente.</li> <li>● <b>true</b>: Detecção completa. Se uma solicitação atingir as condições de bloqueio em Proteção precisa, o WAF não bloqueará a solicitação imediatamente. Em vez disso, ele bloqueia as solicitações até que outras verificações sejam concluídas.</li> </ul>
robot_action	<b>Action</b> object	Ações de proteção para cada regra na proteção anti-crawler.
action	<b>PolicyAction</b> object	Ação Protetora
options	<b>PolicyOption</b> object	Se um tipo de proteção está ativado na política de proteção.
modulex_options	Map<String, Object>	Configurações sobre controle de acesso inteligente. Atualmente, esse recurso ainda está na fase de teste beta aberto (OBT) e disponível em alguns sites.
hosts	Array of strings	Matriz dos ID de nome de domínio protegidas pela política.

Parâmetro	Tipo	Descrição
bind_host	Array of <b>BindHost</b> objects	Matriz de nomes de domínio protegidos com a política de proteção. Comparado com o campo <b>hosts</b> , este campo contém mais detalhes.
extend	Map<String,String>	Campo estendido, que é usado para armazenar a configuração de regras da proteção básica da Web.
timestamp	Long	Hora em que uma política é criada

Tabela 4-177 Ação

Parâmetro	Tipo	Descrição
category	String	Ação de proteção para regras anti-crawler baseadas em recursos: <ul style="list-style-type: none"> <li>● <b>log</b>: O WAF registra apenas os ataques descobertos.</li> <li>● <b>block</b>: WAF bloqueia ataques descobertos.</li> </ul>

Tabela 4-178 PolicyAction

Parâmetro	Tipo	Descrição
category	String	Ação básica de proteção da web. O valor pode ser <b>log</b> ou <b>block</b> . <b>log</b> : WAF apenas registra ataques descobertos. <b>block</b> : WAF bloqueia ataques descobertos. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>block</b></li> <li>● <b>log</b></li> </ul>

Tabela 4-179 PolicyOption

Parâmetro	Tipo	Descrição
webattack	Boolean	Se a proteção básica da Web está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>



Parâmetro	Tipo	Descrição
common	Boolean	Se a verificação geral está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler	Boolean	Este parâmetro é reservado. O valor deste parâmetro é fixado em <b>true</b> . Você pode ignorar esse parâmetro. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_engine	Boolean	Se o motor de busca está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_scanner	Boolean	Se a detecção anti-crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_script	Boolean	Se o JavaScript anti-crawler está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_other	Boolean	Se outra verificação de crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
webshell	Boolean	Se a detecção de webshell está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cc	Boolean	Se as regras de proteção contra ataques da CC estão ativadas Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
custom	Boolean	Se a proteção precisa está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
whiteblackip	Boolean	Se a proteção de blacklist e whitelist está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
geoip	Boolean	Se o controle de acesso de geolocalização está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ignore	Boolean	Se o mascaramento de alarme falso está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
privacy	Boolean	Se o mascaramento de dados está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
antitamper	Boolean	Se a proteção contra adulteração da Web está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
antileakage	Boolean	Se a prevenção de vazamento de informações está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
bot_enable	Boolean	Se a proteção anti-crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
modulex_enabled	Boolean	Se a proteção contra ataques CC para moduleX está ativada. Esse recurso está no teste beta aberto (OBT). Durante o OBT, somente o modo de registro somente é suportado. Valores de enumeração: <ul style="list-style-type: none"> <li>● true</li> <li>● false</li> </ul>

**Tabela 4-180** BindHost

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio
waf_type	String	Modo de implantação da instância do WAF usado para o nome de domínio. O valor pode ser <b>cloud</b> para WAF na nuvem ou <b>premium</b> para instâncias dedicadas do WAF.
mode	String	Este parâmetro é requerido apenas pelo modo dedicado.

**Código de estado: 400**

**Tabela 4-181** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-182** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 403**

**Tabela 4-183** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-184** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**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,
    "gecip" : 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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
403	A cota de recursos é insuficiente.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.3.3 Consulta de uma política por ID

#### Função

Essa API é usada para consultar uma política por ID.

#### URI

GET /v1/{project\_id}/waf/policy/{policy\_id}

**Tabela 4-185** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-186** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-187** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json; charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-188** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da política
name	String	Matriz de detalhes das políticas

Parâmetro	Tipo	Descrição
level	Integer	<p>Nível de proteção da proteção básica da Web</p> <ul style="list-style-type: none"> <li>● <b>1</b>: Baixo. Nesse nível de proteção, o WAF bloqueia apenas solicitações com recursos óbvios de ataque. Se um grande número de alarmes falsos tiver sido relatado, recomenda-se <b>Low</b>.</li> <li>● <b>2</b>: Médio. Esse nível de proteção atende aos requisitos de proteção da Web na maioria dos cenários.</li> <li>● <b>3</b>: Alto. Nesse nível de proteção, o WAF fornece a melhor proteção granular e pode interceptar ataques com recursos complexos de desvio, como ataques cibernéticos Jolokia, detecção de vulnerabilidades de interface de gateway comum (CGI) e ataques de injeção Druid SQL.</li> </ul> <p>Padrão: <b>2</b></p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>1</b></li> <li>● <b>2</b></li> <li>● <b>3</b></li> </ul>
full_detection	Boolean	<p>O modo de detecção em Proteção Precisa.</p> <ul style="list-style-type: none"> <li>● <b>false</b>: Detecção instantânea. Quando uma solicitação atinge as condições de bloqueio na Proteção precisa, o WAF encerra as verificações e bloqueia a solicitação imediatamente.</li> <li>● <b>true</b>: Detecção completa. Se uma solicitação atingir as condições de bloqueio em Proteção precisa, o WAF não bloqueará a solicitação imediatamente. Em vez disso, ele bloqueia as solicitações até que outras verificações sejam concluídas.</li> </ul>
robot_action	<b>Action</b> object	Ações de proteção para cada regra na proteção anti-crawler.
action	<b>PolicyAction</b> object	Ação Protetora
options	<b>PolicyOption</b> object	Se um tipo de proteção está ativado na política de proteção.
modulex_options	Map<String, Object>	Configurações sobre controle de acesso inteligente. Atualmente, esse recurso ainda está na fase de teste beta aberto (OBT) e disponível em alguns sites.
hosts	Array of strings	Matriz dos ID de nome de domínio protegidas pela política.

Parâmetro	Tipo	Descrição
bind_host	Array of <b>BindHost</b> objects	Matriz de nomes de domínio protegidos com a política de proteção. Comparado com o campo <b>hosts</b> , este campo contém mais detalhes.
extend	Map<String,String>	Campo estendido, que é usado para armazenar a configuração de regras da proteção básica da Web.
timestamp	Long	Hora em que uma política é criada

**Tabela 4-189** Ação

Parâmetro	Tipo	Descrição
category	String	Ação de proteção para regras anti-crawler baseadas em recursos: <ul style="list-style-type: none"> <li>● <b>log</b>: O WAF registra apenas os ataques descobertos.</li> <li>● <b>block</b>: WAF bloqueia ataques descobertos.</li> </ul>

**Tabela 4-190** PolicyAction

Parâmetro	Tipo	Descrição
category	String	Ação básica de proteção da web. O valor pode ser <b>log</b> ou <b>block</b> . <b>log</b> : WAF apenas registra ataques descobertos. <b>block</b> : WAF bloqueia ataques descobertos. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>block</b></li> <li>● <b>log</b></li> </ul>

**Tabela 4-191** PolicyOption

Parâmetro	Tipo	Descrição
webattack	Boolean	Se a proteção básica da Web está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>



Parâmetro	Tipo	Descrição
common	Boolean	Se a verificação geral está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler	Boolean	Este parâmetro é reservado. O valor deste parâmetro é fixado em <b>true</b> . Você pode ignorar esse parâmetro. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_engine	Boolean	Se o motor de busca está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_scanner	Boolean	Se a detecção anti-crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_script	Boolean	Se o JavaScript anti-crawler está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_other	Boolean	Se outra verificação de crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
webshell	Boolean	Se a detecção de webshell está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cc	Boolean	Se as regras de proteção contra ataques da CC estão ativadas Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
custom	Boolean	Se a proteção precisa está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
whiteblackip	Boolean	Se a proteção de blacklist e whitelist está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
geoip	Boolean	Se o controle de acesso de geolocalização está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
ignore	Boolean	Se o mascaramento de alarme falso está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
privacy	Boolean	Se o mascaramento de dados está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
antitamper	Boolean	Se a proteção contra adulteração da Web está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
antileakage	Boolean	Se a prevenção de vazamento de informações está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
bot_enable	Boolean	Se a proteção anti-crawler está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>

Parâmetro	Tipo	Descrição
modulex_enabled	Boolean	Se a proteção contra ataques CC para moduleX está ativada. Esse recurso está no teste beta aberto (OBT). Durante o OBT, somente o modo de registro somente é suportado. Valores de enumeração: <ul style="list-style-type: none"> <li>● true</li> <li>● false</li> </ul>

**Tabela 4-192** BindHost

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio
waf_type	String	Modo de implantação da instância do WAF usado para o nome de domínio. O valor pode ser <b>cloud</b> para WAF na nuvem ou <b>premium</b> para instâncias dedicadas do WAF.
mode	String	Este parâmetro é requerido apenas pelo modo dedicado.

**Código de estado: 400**

**Tabela 4-193** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-194** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-195** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**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,
    "whiteblackip" : true,
    "gecip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "antileakage" : false,
    "bot_enable" : true,
    "modulex_enabled" : false
  },
  "hosts" : [ ],
  "extend" : { },
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ ]
}
```

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.

Código de status	Descrição
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.3.4 Atualização de uma política de proteção

#### Função

Esta API é usada para atualizar uma política. O corpo da solicitação pode conter apenas a parte a ser atualizada.

#### URI

PATCH /v1/{project\_id}/waf/policy/{policy\_id}

**Tabela 4-196** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-197** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-198** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-199** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
name	Não	String	Matriz de detalhes das políticas
level	Não	Integer	<p>Nível de proteção da proteção básica da Web</p> <ul style="list-style-type: none"> <li>● <b>1</b>: Baixo. Nesse nível de proteção, o WAF bloqueia apenas solicitações com recursos óbvios de ataque. Se um grande número de alarmes falsos tiver sido relatado, recomenda-se <b>Low</b>.</li> <li>● <b>2</b>: Médio. Esse nível de proteção atende aos requisitos de proteção da Web na maioria dos cenários.</li> <li>● <b>3</b>: Alto. Nesse nível de proteção, o WAF fornece a melhor proteção granular e pode interceptar ataques com recursos complexos de desvio, como ataques cibernéticos Jolokia, detecção de vulnerabilidades de interface de gateway comum (CGI) e ataques de injeção Druid SQL.</li> </ul> <p>Padrão: <b>2</b></p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>1</b></li> <li>● <b>2</b></li> <li>● <b>3</b></li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
full_detection	Não	Boolean	<p>O modo de detecção em Proteção Precisa.</p> <ul style="list-style-type: none"> <li>● <b>false</b>: Detecção instantânea. Quando uma solicitação atinge as condições de bloqueio na Proteção precisa, o WAF encerra as verificações e bloqueia a solicitação imediatamente.</li> <li>● <b>true</b>: Detecção completa. Se uma solicitação atingir as condições de bloqueio em Proteção precisa, o WAF não bloqueará a solicitação imediatamente. Em vez disso, ele bloqueia as solicitações até que outras verificações sejam concluídas.</li> </ul>
robot_action	Não	<b>Action</b> object	Ações de proteção para cada regra na proteção anti-crawler.
action	Não	<b>PolicyAction</b> object	Ação Protetora
options	Não	<b>PolicyOption</b> object	Se um tipo de proteção está ativado na política de proteção.
modulex_options	Não	Map<String, Object>	Configurações sobre controle de acesso inteligente. Atualmente, esse recurso ainda está na fase de teste beta aberto (OBT) e disponível em alguns sites.
hosts	Não	Array of strings	Matriz dos ID de nome de domínio protegidas pela política.
bind_host	Não	Array of <b>BindHost</b> objects	Matriz de nomes de domínio protegidos com a política de proteção. Comparado com o campo <b>hosts</b> , este campo contém mais detalhes.
extend	Não	Map<String, String>	Campo estendido, que é usado para armazenar a configuração de regras da proteção básica da Web.

**Tabela 4-200** Ação

Parâmetro	Obrigatório	Tipo	Descrição
category	Não	String	Ação de proteção para regras anti-crawler baseadas em recursos: <ul style="list-style-type: none"> <li>● <b>log</b>: O WAF registra apenas os ataques descobertos.</li> <li>● <b>block</b>: WAF bloqueia ataques descobertos.</li> </ul>

**Tabela 4-201** PolicyAction

Parâmetro	Obrigatório	Tipo	Descrição
category	Não	String	Ação básica de proteção da web. O valor pode ser <b>log</b> ou <b>block</b> . <b>log</b> : WAF apenas registra ataques descobertos. <b>block</b> : WAF bloqueia ataques descobertos. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>block</b></li> <li>● <b>log</b></li> </ul>

**Tabela 4-202** PolicyOption

Parâmetro	Obrigatório	Tipo	Descrição
webattack	Não	Boolean	Se a proteção básica da Web está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
common	Não	Boolean	Se a verificação geral está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler	Não	Boolean	Este parâmetro é reservado. O valor deste parâmetro é fixado em <b>true</b> . Você pode ignorar esse parâmetro. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>



Parâmetro	Obrigatório	Tipo	Descrição
crawler_engine	Não	Boolean	Se o motor de busca está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
crawler_scanner	Não	Boolean	Se a detecção anti-crawler está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
crawler_script	Não	Boolean	Se o JavaScript anti-crawler está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
crawler_other	Não	Boolean	Se outra verificação de crawler está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
webshell	Não	Boolean	Se a detecção de webshell está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
cc	Não	Boolean	Se as regras de proteção contra ataques da CC estão ativadas Valores de enumeração: ● <b>true</b> ● <b>false</b>
custom	Não	Boolean	Se a proteção precisa está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
whiteblackip	Não	Boolean	Se a proteção de blacklist e whitelist está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>

Parâmetro	Obrigatório	Tipo	Descrição
geoip	Não	Boolean	Se o controle de acesso de geolocalização está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
ignore	Não	Boolean	Se o mascaramento de alarme falso está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
privacy	Não	Boolean	Se o mascaramento de dados está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
antitamper	Não	Boolean	Se a proteção contra adulteração da Web está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
antileakage	Não	Boolean	Se a prevenção de vazamento de informações está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
bot_enable	Não	Boolean	Se a proteção anti-crawler está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
modulex_enabled	Não	Boolean	Se a proteção contra ataques CC para moduleX está ativada. Esse recurso está no teste beta aberto (OBT). Durante o OBT, somente o modo de registro somente é suportado. Valores de enumeração: ● <b>true</b> ● <b>false</b>

**Tabela 4-203** BindHost

Parâmetro	Obrigatório	Tipo	Descrição
id	Não	String	ID do nome de domínio
hostname	Não	String	Nome de domínio
waf_type	Não	String	Modo de implantação da instância do WAF usado para o nome de domínio. O valor pode ser <b>cloud</b> para WAF na nuvem ou <b>premium</b> para instâncias dedicadas do WAF.
mode	Não	String	Este parâmetro é requerido apenas pelo modo dedicado.

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-204** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da política
name	String	Matriz de detalhes das políticas
level	Integer	<p>Nível de proteção da proteção básica da Web</p> <ul style="list-style-type: none"> <li>● <b>1:</b> Baixo. Nesse nível de proteção, o WAF bloqueia apenas solicitações com recursos óbvios de ataque. Se um grande número de alarmes falsos tiver sido relatado, recomenda-se <b>Low</b>.</li> <li>● <b>2:</b> Médio. Esse nível de proteção atende aos requisitos de proteção da Web na maioria dos cenários.</li> <li>● <b>3:</b> Alto. Nesse nível de proteção, o WAF fornece a melhor proteção granular e pode interceptar ataques com recursos complexos de desvio, como ataques cibernéticos Jolokia, detecção de vulnerabilidades de interface de gateway comum (CGI) e ataques de injeção Druid SQL.</li> </ul> <p>Padrão: <b>2</b></p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>1</b></li> <li>● <b>2</b></li> <li>● <b>3</b></li> </ul>

Parâmetro	Tipo	Descrição
full_detection	Boolean	O modo de detecção em Proteção Precisa. <ul style="list-style-type: none"> <li>● <b>false</b>: Detecção instantânea. Quando uma solicitação atinge as condições de bloqueio na Proteção precisa, o WAF encerra as verificações e bloqueia a solicitação imediatamente.</li> <li>● <b>true</b>: Detecção completa. Se uma solicitação atingir as condições de bloqueio em Proteção precisa, o WAF não bloqueará a solicitação imediatamente. Em vez disso, ele bloqueia as solicitações até que outras verificações sejam concluídas.</li> </ul>
robot_action	<b>Action</b> object	Ações de proteção para cada regra na proteção anti-crawler.
action	<b>PolicyAction</b> object	Ação Protetora
options	<b>PolicyOption</b> object	Se um tipo de proteção está ativado na política de proteção.
modulex_options	Map<String, Object>	Configurações sobre controle de acesso inteligente. Atualmente, esse recurso ainda está na fase de teste beta aberto (OBT) e disponível em alguns sites.
hosts	Array of strings	Matriz dos ID de nome de domínio protegidas pela política.
bind_host	Array of <b>BindHost</b> objects	Matriz de nomes de domínio protegidos com a política de proteção. Comparado com o campo <b>hosts</b> , este campo contém mais detalhes.
extend	Map<String, String>	Campo estendido, que é usado para armazenar a configuração de regras da proteção básica da Web.
timestamp	Long	Hora em que uma política é criada

**Tabela 4-205** Ação

Parâmetro	Tipo	Descrição
category	String	Ação de proteção para regras anti-crawler baseadas em recursos: <ul style="list-style-type: none"> <li>● <b>log</b>: O WAF registra apenas os ataques descobertos.</li> <li>● <b>block</b>: WAF bloqueia ataques descobertos.</li> </ul>

**Tabela 4-206** PolicyAction

Parâmetro	Tipo	Descrição
category	String	<p>Ação básica de proteção da web. O valor pode ser <b>log</b> ou <b>block</b>. <b>log</b>: WAF apenas registra ataques descobertos. <b>block</b>: WAF bloqueia ataques descobertos.</p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>block</b></li> <li>● <b>log</b></li> </ul>

**Tabela 4-207** PolicyOption

Parâmetro	Tipo	Descrição
webattack	Boolean	<p>Se a proteção básica da Web está ativada</p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
common	Boolean	<p>Se a verificação geral está ativada</p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler	Boolean	<p>Este parâmetro é reservado. O valor deste parâmetro é fixado em <b>true</b>. Você pode ignorar esse parâmetro.</p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_engine	Boolean	<p>Se o motor de busca está ativado</p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_scanner	Boolean	<p>Se a detecção anti-crawler está ativada</p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_script	Boolean	<p>Se o JavaScript anti-crawler está ativado</p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
crawler_other	Boolean	Se outra verificação de crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
webshell	Boolean	Se a detecção de webshell está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cc	Boolean	Se as regras de proteção contra ataques da CC estão ativadas Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
custom	Boolean	Se a proteção precisa está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
whiteblackip	Boolean	Se a proteção de lista negra e lista branca está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
geoip	Boolean	Se o controle de acesso de geolocalização está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ignore	Boolean	Se o mascaramento de alarme falso está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
privacy	Boolean	Se o mascaramento de dados está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
antitamper	Boolean	Se a proteção contra adulteração da Web está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
antileakage	Boolean	Se a prevenção de vazamento de informações está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
bot_enable	Boolean	Se a proteção anti-crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
modulex_enabled	Boolean	Se a proteção contra ataques CC para moduleX está ativada. Esse recurso está no teste beta aberto (OBT). Durante o OBT, somente o modo de registro somente é suportado. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

**Tabela 4-208** BindHost

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio
waf_type	String	Modo de implantação da instância do WAF usado para o nome de domínio. O valor pode ser <b>cloud</b> para WAF na nuvem ou <b>premium</b> para instâncias dedicadas do WAF.
mode	String	Este parâmetro é requerido apenas pelo modo dedicado.

**Código de estado: 400**

**Tabela 4-209** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-210** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-211** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

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

## Exemplo de respostas

**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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.3.5 Exclusão de uma política de proteção

#### Função

Esta API é usada para excluir uma política de proteção. Se a política estiver em uso, desvincule o nome de domínio da política antes de excluir a política.

## URI

DELETE /v1/{project\_id}/waf/policy/{policy\_id}

**Tabela 4-212** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-213** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-214** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json; charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-215** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da política
name	String	Matriz de detalhes das políticas
level	Integer	<p>Nível de proteção da proteção básica da Web</p> <ul style="list-style-type: none"> <li>● <b>1</b>: Baixo. Nesse nível de proteção, o WAF bloqueia apenas solicitações com recursos óbvios de ataque. Se um grande número de alarmes falsos tiver sido relatado, recomenda-se <b>Low</b>.</li> <li>● <b>2</b>: Médio. Esse nível de proteção atende aos requisitos de proteção da Web na maioria dos cenários.</li> <li>● <b>3</b>: Alto. Nesse nível de proteção, o WAF fornece a melhor proteção granular e pode interceptar ataques com recursos complexos de desvio, como ataques cibernéticos Jolokia, detecção de vulnerabilidades de interface de gateway comum (CGI) e ataques de injeção Druid SQL.</li> </ul> <p>Padrão: <b>2</b></p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>1</b></li> <li>● <b>2</b></li> <li>● <b>3</b></li> </ul>
full_detection	Boolean	<p>O modo de detecção em Proteção Precisa.</p> <ul style="list-style-type: none"> <li>● <b>false</b>: Detecção instantânea. Quando uma solicitação atinge as condições de bloqueio na Proteção precisa, o WAF encerra as verificações e bloqueia a solicitação imediatamente.</li> <li>● <b>true</b>: Detecção completa. Se uma solicitação atingir as condições de bloqueio em Proteção precisa, o WAF não bloqueará a solicitação imediatamente. Em vez disso, ele bloqueia as solicitações até que outras verificações sejam concluídas.</li> </ul>
robot_action	<b>Action</b> object	Ações de proteção para cada regra na proteção anti-crawler.
action	<b>PolicyAction</b> object	Ação Protetora
options	<b>PolicyOption</b> object	Se um tipo de proteção está ativado na política de proteção.
modulex_options	Map<String, Object>	Configurações sobre controle de acesso inteligente. Atualmente, esse recurso ainda está na fase de teste beta aberto (OBT) e disponível em alguns sites.

Parâmetro	Tipo	Descrição
hosts	Array of strings	Matriz dos ID de nome de domínio protegidas pela política.
bind_host	Array of <b>BindHost</b> objects	Matriz de nomes de domínio protegidos com a política de proteção. Comparado com o campo <b>hosts</b> , este campo contém mais detalhes.
extend	Map<String,String>	Campo estendido, que é usado para armazenar a configuração de regras da proteção básica da Web.
timestamp	Long	Hora em que uma política é criada

Tabela 4-216 Ação

Parâmetro	Tipo	Descrição
category	String	Ação de proteção para regras anti-crawler baseadas em recursos: <ul style="list-style-type: none"> <li>● <b>log</b>: O WAF registra apenas os ataques descobertos.</li> <li>● <b>block</b>: WAF bloqueia ataques descobertos.</li> </ul>

Tabela 4-217 PolicyAction

Parâmetro	Tipo	Descrição
category	String	Ação básica de proteção da web. O valor pode ser <b>log</b> ou <b>block</b> . <b>log</b> : WAF apenas registra ataques descobertos. <b>block</b> : WAF bloqueia ataques descobertos. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>block</b></li> <li>● <b>log</b></li> </ul>

Tabela 4-218 PolicyOption

Parâmetro	Tipo	Descrição
webattack	Boolean	Se a proteção básica da Web está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
common	Boolean	Se a verificação geral está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler	Boolean	Este parâmetro é reservado. O valor deste parâmetro é fixado em <b>true</b> . Você pode ignorar esse parâmetro. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_engine	Boolean	Se o motor de busca está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_scanner	Boolean	Se a detecção anti-crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_script	Boolean	Se o JavaScript anti-crawler está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_other	Boolean	Se outra verificação de crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
webshell	Boolean	Se a detecção de webshell está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cc	Boolean	Se as regras de proteção contra ataques da CC estão ativadas Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
custom	Boolean	Se a proteção precisa está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
whiteblackip	Boolean	Se a proteção de blacklist e whitelist está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
geoip	Boolean	Se o controle de acesso de geolocalização está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
ignore	Boolean	Se o mascaramento de alarme falso está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
privacy	Boolean	Se o mascaramento de dados está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
antitamper	Boolean	Se a proteção contra adulteração da Web está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
antileakage	Boolean	Se a prevenção de vazamento de informações está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
bot_enable	Boolean	Se a proteção anti-crawler está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>

Parâmetro	Tipo	Descrição
modulex_enabled	Boolean	Se a proteção contra ataques CC para moduleX está ativada. Esse recurso está no teste beta aberto (OBT). Durante o OBT, somente o modo de registro somente é suportado. Valores de enumeração: <ul style="list-style-type: none"> <li>● true</li> <li>● false</li> </ul>

**Tabela 4-219 BindHost**

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio
waf_type	String	Modo de implantação da instância do WAF usado para o nome de domínio. O valor pode ser <b>cloud</b> para WAF na nuvem ou <b>premium</b> para instâncias dedicadas do WAF.
mode	String	Este parâmetro é requerido apenas pelo modo dedicado.

**Código de estado: 400**

**Tabela 4-220** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-221** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-222** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

Solicitação bem-sucedida.

```
{
  "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,
    "gecip" : 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 status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.3.6 Atualização da política de proteção de nomes de domínio

#### Função

Essa API é usada para atualizar a política de proteção aplicada a um nome de domínio.

#### URI

PUT /v1/{project\_id}/waf/policy/{policy\_id}

**Tabela 4-223** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-224** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial.

Parâmetro	Obrigatório	Tipo	Descrição
hosts	Sim	String	ID do nome de domínio. Ele pode ser obtido chamando a API <b>ListHost</b> .

## Parâmetros de solicitação

**Tabela 4-225** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json; charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-226** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da política
name	String	Matriz de detalhes das políticas

Parâmetro	Tipo	Descrição
level	Integer	<p>Nível de proteção da proteção básica da Web</p> <ul style="list-style-type: none"> <li>● <b>1</b>: Baixo. Nesse nível de proteção, o WAF bloqueia apenas solicitações com recursos óbvios de ataque. Se um grande número de alarmes falsos tiver sido relatado, recomenda-se <b>Low</b>.</li> <li>● <b>2</b>: Médio. Esse nível de proteção atende aos requisitos de proteção da Web na maioria dos cenários.</li> <li>● <b>3</b>: Alto. Nesse nível de proteção, o WAF fornece a melhor proteção granular e pode interceptar ataques com recursos complexos de desvio, como ataques cibernéticos Jolokia, detecção de vulnerabilidades de interface de gateway comum (CGI) e ataques de injeção Druid SQL.</li> </ul> <p>Padrão: <b>2</b></p> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>1</b></li> <li>● <b>2</b></li> <li>● <b>3</b></li> </ul>
full_detection	Boolean	<p>O modo de detecção em Proteção Precisa.</p> <ul style="list-style-type: none"> <li>● <b>false</b>: Detecção instantânea. Quando uma solicitação atinge as condições de bloqueio na Proteção precisa, o WAF encerra as verificações e bloqueia a solicitação imediatamente.</li> <li>● <b>true</b>: Detecção completa. Se uma solicitação atingir as condições de bloqueio em Proteção precisa, o WAF não bloqueará a solicitação imediatamente. Em vez disso, ele bloqueia as solicitações até que outras verificações sejam concluídas.</li> </ul>
robot_action	<b>Action</b> object	Ações de proteção para cada regra na proteção anti-crawler.
action	<b>PolicyAction</b> object	Ação Protetora
options	<b>PolicyOption</b> object	Se um tipo de proteção está ativado na política de proteção.
modulex_options	Map<String, Object>	Configurações sobre controle de acesso inteligente. Atualmente, esse recurso ainda está na fase de teste beta aberto (OBT) e disponível em alguns sites.
hosts	Array of strings	Matriz dos ID de nome de domínio protegidas pela política.

Parâmetro	Tipo	Descrição
bind_host	Array of <b>BindHost</b> objects	Matriz de nomes de domínio protegidos com a política de proteção. Comparado com o campo <b>hosts</b> , este campo contém mais detalhes.
extend	Map<String,String>	Campo estendido, que é usado para armazenar a configuração de regras da proteção básica da Web.
timestamp	Long	Hora em que uma política é criada

Tabela 4-227 Ação

Parâmetro	Tipo	Descrição
category	String	Ação de proteção para regras anti-crawler baseadas em recursos: <ul style="list-style-type: none"> <li>● <b>log</b>: O WAF registra apenas os ataques descobertos.</li> <li>● <b>block</b>: WAF bloqueia ataques descobertos.</li> </ul>

Tabela 4-228 PolicyAction

Parâmetro	Tipo	Descrição
category	String	Ação básica de proteção da web. O valor pode ser <b>log</b> ou <b>block</b> . <b>log</b> : WAF apenas registra ataques descobertos. <b>block</b> : WAF bloqueia ataques descobertos. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>block</b></li> <li>● <b>log</b></li> </ul>

Tabela 4-229 PolicyOption

Parâmetro	Tipo	Descrição
webattack	Boolean	Se a proteção básica da Web está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
common	Boolean	Se a verificação geral está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler	Boolean	Este parâmetro é reservado. O valor deste parâmetro é fixado em <b>true</b> . Você pode ignorar esse parâmetro. Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_engine	Boolean	Se o motor de busca está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_scanner	Boolean	Se a detecção anti-crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_script	Boolean	Se o JavaScript anti-crawler está ativado Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
crawler_other	Boolean	Se outra verificação de crawler está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
webshell	Boolean	Se a detecção de webshell está ativada Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cc	Boolean	Se as regras de proteção contra ataques da CC estão ativadas Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

Parâmetro	Tipo	Descrição
custom	Boolean	Se a proteção precisa está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
whiteblackip	Boolean	Se a proteção de blacklist e whitelist está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
geoip	Boolean	Se o controle de acesso de geolocalização está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
ignore	Boolean	Se o mascaramento de alarme falso está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
privacy	Boolean	Se o mascaramento de dados está ativado Valores de enumeração: ● <b>true</b> ● <b>false</b>
antitamper	Boolean	Se a proteção contra adulteração da Web está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
antileakage	Boolean	Se a prevenção de vazamento de informações está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>
bot_enable	Boolean	Se a proteção anti-crawler está ativada Valores de enumeração: ● <b>true</b> ● <b>false</b>

Parâmetro	Tipo	Descrição
modulex_enabled	Boolean	Se a proteção contra ataques CC para moduleX está ativada. Esse recurso está no teste beta aberto (OBT). Durante o OBT, somente o modo de registro somente é suportado. Valores de enumeração: <ul style="list-style-type: none"> <li>● true</li> <li>● false</li> </ul>

**Tabela 4-230 BindHost**

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio
waf_type	String	Modo de implantação da instância do WAF usado para o nome de domínio. O valor pode ser <b>cloud</b> para WAF na nuvem ou <b>premium</b> para instâncias dedicadas do WAF.
mode	String	Este parâmetro é requerido apenas pelo modo dedicado.

**Código de estado: 400**

**Tabela 4-231** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-232** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-233** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**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,
    "geoup" : 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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

# 4.4 Gerenciamento de regras

## 4.4.1 Alteração de status de uma regra

### Função

Essa API é usada para alterar o status de uma única regra, por exemplo, desativando uma regra de Proteção precisa.

### URI

PUT /v1/{project\_id}/waf/policy/{policy\_id}/{ruletype}/{rule\_id}/status

**Tabela 4-234** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API para consultar a lista de políticas.

Parâmetro	Obrigatório	Tipo	Descrição
ruletype	Sim	String	Tipo de política Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>whiteblackip</b></li> <li>● <b>geoip</b></li> <li>● <b>privacy</b></li> <li>● <b>antitamper</b></li> <li>● <b>custom</b></li> <li>● <b>ignore</b></li> </ul>
rule_id	Sim	String	ID da regra. Ele pode ser obtido chamando a API específica que é usada para obter a lista de regras de um determinado tipo. Por exemplo, você pode chamar a API <b>ListWhiteblackipRule</b> para obter o ID de uma regra de lista negra ou de lista branca.

**Tabela 4-235** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-236** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-237** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
status	Não	Integer	Estado. As opções são <b>0</b> e <b>1</b> . <b>0</b> : Desabilitado. <b>1</b> : Ativado.

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-238** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
policyid	String	ID da política
timestamp	Long	Hora em que a regra foi criada.
description	String	Descrição da regra
status	Integer	Estado. As opções são <b>0</b> e <b>1</b> . <b>0</b> : Desabilitado. <b>1</b> : Ativado.

**Código de estado: 400**

**Tabela 4-239** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-240** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-241** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

OK

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

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.4.2 Consulta de regras da lista branca de proteção global (Anteriormente mascaramento de alarmes falsos)

### Função

Consulta de regras da lista branca de proteção global (Anteriormente mascaramento de alarmes falsos)

## URI

GET /v1/{project\_id}/waf/policy/{policy\_id}/ignore

**Tabela 4-242** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-243** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.
page	Não	Integer	Número de página dos dados a serem retornados durante a consulta de paginação. O valor padrão é <b>1</b> , indicando que os dados na primeira página são retornados. Padrão: <b>1</b>
pagesize	Não	Integer	Número de resultados em cada página durante a consulta de paginação. Faixa de valor: <b>1</b> a <b>100</b> . O valor padrão é <b>10</b> , indicando que cada página contém 10 resultados. Padrão: <b>10</b>

## Parâmetros de solicitação

**Tabela 4-244** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-245** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	O número de regras de lista branca de proteção global (anteriormente mascaramento de alarme falso) na política de proteção.
items	Array of <b>IgnoreRuleBody</b> objects	Nomes de domínio para os quais a regra de lista branca de proteção global (anteriormente mascaramento de alarme falso) é usada.

**Tabela 4-246** IgnoreRuleBody

Parâmetro	Tipo	Descrição
id	String	ID da regra
policyid	String	ID da política de proteção que inclui a regra
timestamp	Long	Timestamp a regra foi criada.
description	String	Descrição da regra
status	Integer	Status da regra. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: A regra está desativada.</li> <li>● <b>1</b>: A regra está ativada.</li> </ul>
url	String	O caminho para falsos alarmes de mascaramento. Este parâmetro só está disponível quando <b>mode</b> está definido como <b>0</b> .

Parâmetro	Tipo	Descrição
rule	String	<p>Regras a serem mascaradas</p> <ul style="list-style-type: none"> <li>● Se você quiser bloquear uma regra interna específica, o valor desse parâmetro é o ID da regra. Para consultar a ID da regra, vá para o console do WAF, escolha <b>Policies</b> e clique no nome da política de destino. Na página exibida, na área <b>Basic Web Protection</b>, selecione a guia <b>Protection Rules</b> e exiba a ID da regra específica. Você também pode consultar a ID da regra nos detalhes do evento.</li> <li>● Se você quiser mascarar um tipo de regras básicas de proteção da Web, defina esse parâmetro como o nome do tipo de regras básicas de proteção da Web. <b>xss</b>: XSS ataca <b>webshell</b>: Web shells <b>vuln</b>: Outros tipos de ataques <b>sql</b>: <b>robot</b> de ataque de injeção SQL: Rastreadores maliciosos <b>rfi</b>: Inclusão de arquivo remoto <b>lfi</b>: Inclusão de arquivo local <b>cmdi</b>: Ataque de injeção de comando</li> <li>● Para ignorar a proteção básica da Web, defina esse parâmetro como <b>all</b>.</li> <li>● Para ignorar toda a proteção de WAF, defina este parâmetro para <b>bypass</b>.</li> </ul>
mode	Integer	Número da versão. O valor 0 indica a versão antiga V1 e o valor 1 indica a nova versão V2. Se o valor de mode for 0, o campo de condições não existe, e os campos url e url_logic existem. Quando o valor de mode é 1, os campos url e url_logic não existem, e o campo de condições existe.
url_logic	String	Correspondência lógica. O valor pode ser <b>equal</b> , <b>not_equal</b> , <b>contain</b> , <b>not_contain</b> , <b>prefix</b> , <b>not_prefix</b> , <b>suffix</b> , <b>not_suffix</b> .
conditions	Array of <b>Condition</b> objects	Lista de Condição
domain	Array of strings	Protegendo nomes de domínio ou protegendo sites
advanced	Array of <b>Advanced</b> objects	Configurações avançadas

**Tabela 4-247** Condição

Parâmetro	Tipo	Descrição
category	String	Tipo de campo. O valor pode ser <b>ip</b> , <b>url</b> , <b>params</b> , <b>cookie</b> , ou <b>header</b> .
contents	Array of strings	Conteúdo. O comprimento da matriz deve ser 1. O formato do conteúdo varia de acordo com os tipos de campo. Por exemplo, se o tipo de campo for <b>ip</b> , o valor deverá ser um endereço IP ou intervalo de endereços IP. Se o tipo de campo for <b>url</b> , o valor deve ser um URL no formato padrão. Se o tipo de campo for <b>parâmetros</b> , <b>cookie</b> ou <b>cabeçalho</b> , o formato do conteúdo não é limitado.
logic_operation	String	A lógica de correspondência varia dependendo do tipo de campo. Por exemplo, se o tipo de campo for <b>ip</b> , a lógica pode ser <b>equal</b> ou <b>not_equal</b> . Se o tipo do campo for <b>url</b> , <b>params</b> , <b>cookie</b> , ou <b>header</b> , a lógica pode ser <b>equal</b> , <b>not_equal</b> , <b>contain</b> , <b>not_contain</b> , <b>prefix</b> , <b>not_prefix</b> , <b>suffix</b> , <b>not_suffix</b> .
check_all_indexes_logic	Integer	Este parâmetro é reservado e pode ser ignorado.
index	String	Se o tipo de campo for <b>ip</b> e o subcampo for o endereço IP do cliente, o parâmetro <b>index</b> não existirá. Se o tipo de subcampo for <b>X-Forwarded-For</b> , o valor será <b>x-forwarded-for</b> . Se o tipo de campo for <b>params</b> , <b>header</b> , ou <b>cookie</b> , e o subcampo for definido pelo usuário, o valor de <b>index</b> será o subcampo definido pelo usuário.

**Tabela 4-248** Avançado

Parâmetro	Tipo	Descrição
index	String	Tipo de campo. Os seguintes tipos de campo são suportados: <b>Params</b> , <b>Cookie</b> , <b>Header</b> , <b>Body</b> e <b>Multipart</b> . <ul style="list-style-type: none"> <li>● Ao selecionar <b>Params</b>, <b>Cookie</b>, ou <b>Header</b>, você pode definir esse parâmetro para <b>all</b> ou configurar subcampos conforme necessário.</li> <li>● Quando você seleciona <b>Body</b> ou <b>Multipart</b>, defina este parâmetro como <b>all</b>.</li> </ul>
contentsts	Array of strings	Subcampo do tipo de campo especificado. O valor padrão é <b>all</b> .

**Código de estado: 400**



**Tabela 4-249** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 403**

**Tabela 4-250** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-251** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-252** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
403	Cota de recurso insuficiente.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.4.3 Criação de uma regra de lista branca de proteção global (Anteriormente mascaramento de alarme falso)

#### Função

Criação de uma regra de lista branca de proteção global (Anteriormente mascaramento de alarme falso)

#### URI

POST /v1/{project\_id}/waf/policy/{policy\_id}/ignore

**Tabela 4-253** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-254** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-255** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-256** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
domain	Sim	Array of strings	Nome de domínio ou site a ser protegido. Se o comprimento da matriz for <b>0</b> , a regra entrará em vigor para todos os nomes de domínio ou sites.

Parâmetro	Obrigatório	Tipo	Descrição
conditions	Sim	Array of <b>CreateCondition</b> objects	Lista de Condição
mode	Sim	Integer	O valor é fixado em <b>1</b> , indicando regras de mascaramento de alarme falso v2. A v1 é usada apenas para compatibilidade com versões anteriores, e as regras de alarme falso não podem ser criadas na v1.
rule	Sim	String	<p>Itens a serem mascarados. Você pode fornecer vários itens e separá-los com ponto e vírgula (;).</p> <ul style="list-style-type: none"> <li>● Se você quiser bloquear uma regra interna específica, o valor desse parâmetro é o ID da regra. Para consultar a ID da regra, vá para o console do WAF, escolha <b>Policies</b> e clique no nome da política de destino. Na página exibida, na área <b>Basic Web Protection</b>, selecione a guia <b>Protection Rules</b> e exiba a ID da regra específica. Você também pode consultar a ID da regra nos detalhes do evento.</li> <li>● Se você quiser mascarar um tipo de regras básicas de proteção da Web, defina esse parâmetro como o nome do tipo de regras básicas de proteção da Web. <b>xss</b>: XSS ataca <b>webshell</b>: Web shells <b>vuln</b>: Outros tipos de ataques <b>sql</b>: <b>robot</b> de ataque de injeção SQL: Rastreadores maliciosos <b>rfi</b>: Inclusão de arquivo remoto <b>lfi</b>: Inclusão de arquivo local <b>cmdi</b>: Ataque de injeção de comando</li> <li>● Para ignorar a proteção básica da Web, defina esse parâmetro como <b>all</b>.</li> <li>● Para ignorar toda a proteção de WAF, defina este parâmetro para <b>bypass</b>.</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
advanced	Não	Array of <b>Advanced</b> objects	Configurações avançadas
description	Não	String	Descrição de uma regra de mascaramento

**Tabela 4-257** CreateCondition

Parâmetro	Obrigatório	Tipo	Descrição
category	Sim	String	Tipo de campo. O valor pode ser <b>ip</b> , <b>url</b> , <b>params</b> , <b>cookie</b> , ou <b>header</b> .
contents	Sim	Array of strings	Conteúdo. O comprimento da matriz é limitado a <b>1</b> . O formato do conteúdo varia dependendo do tipo de campo. Por exemplo, se o tipo de campo for <b>ip</b> , o valor deverá ser um endereço IP ou intervalo de endereços IP. Se o tipo de campo for <b>url</b> , o valor deve estar no formato de URL padrão. Se o tipo de campo for <b>params</b> , <b>cookie</b> , ou <b>header</b> , o formato do conteúdo não é limitado.
logic_operation	Sim	String	A lógica de correspondência varia dependendo do tipo de campo. Por exemplo, se o tipo de campo for <b>ip</b> , a lógica pode ser <b>equal</b> ou <b>not_equal</b> . Se o tipo do campo for <b>url</b> , <b>params</b> , <b>cookie</b> , ou <b>header</b> , a lógica pode ser <b>equal</b> , <b>not_equal</b> , <b>contain</b> , <b>not_contain</b> , <b>prefix</b> , <b>not_prefix</b> , <b>suffix</b> , <b>not_suffix</b> .
check_all_indexes_logic	Não	Integer	Este parâmetro é reservado e pode ser ignorado.

Parâmetro	Obrigatório	Tipo	Descrição
index	Não	String	Se o tipo de campo for <b>ip</b> e o subcampo for o endereço IP do cliente, o parâmetro <b>index</b> não será necessário. Se o tipo de subcampo for <b>X-Forwarded-For</b> , o valor será <b>x-forwarded-for</b> . Se o tipo de campo for <b>params</b> , <b>header</b> , ou <b>cookie</b> , e o subcampo for definido pelo usuário, o valor do <b>index</b> será o subcampo definido pelo usuário.

Tabela 4-258 Avançado

Parâmetro	Obrigatório	Tipo	Descrição
index	Não	String	Tipo de campo. Os seguintes tipos de campo são suportados: Params, Cookie, Header, Body e Multipart. <ul style="list-style-type: none"> <li>● Ao selecionar <b>Params</b>, <b>Cookie</b>, ou <b>Header</b>, você pode definir esse parâmetro para <b>all</b> ou configurar subcampos conforme necessário.</li> <li>● Quando você seleciona <b>Body</b> ou <b>Multipart</b>, defina este parâmetro como <b>all</b>.</li> </ul>
contensts	Não	Array of strings	Subcampo do tipo de campo especificado. O valor padrão é <b>all</b> .

## Parâmetros de resposta

**Código de estado: 200**

Tabela 4-259 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
policyid	String	ID da política
timestamp	Long	Timestamp a regra foi criada.
description	String	Descrição da regra

Parâmetro	Tipo	Descrição
status	Integer	Status da regra. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: A regra está desativada.</li> <li>● <b>1</b>: A regra está ativada.</li> </ul>
rule	String	ID da regra incorporada a ser mascarada. Você pode consultar a ID da regra escolhendo <b>Policies &gt; Policy Name &gt; Basic Web Protection &gt; Protection Rules</b> no console do WAF ou na página de detalhes do evento.
mode	Integer	O valor é fixado em <b>1</b> , indicando que as regras de mascaramento de alarme falso v2 são usadas. A v1 é usada apenas para compatibilidade com versões anteriores, e as regras de alarme falso não podem ser criadas na v1.
conditions	Array of <b>Condition</b> objects	Lista de Condição
advanced	Array of <b>Advanced</b> objects	Configurações avançadas
domain	Array of strings	Nome de domínio ou site protegido

**Tabela 4-260** Condição

Parâmetro	Tipo	Descrição
category	String	Tipo de campo. O valor pode ser <b>ip</b> , <b>url</b> , <b>params</b> , <b>cookie</b> , ou <b>header</b> .
contents	Array of strings	Conteúdo. O comprimento da matriz deve ser 1. O formato do conteúdo varia de acordo com os tipos de campo. Por exemplo, se o tipo de campo for <b>ip</b> , o valor deverá ser um endereço IP ou intervalo de endereços IP. Se o tipo de campo for <b>url</b> , o valor deve ser um URL no formato padrão. Se o tipo de campo for parâmetros, cookie ou cabeçalho, o formato do conteúdo não é limitado.
logic_operation	String	A lógica de correspondência varia dependendo do tipo de campo. Por exemplo, se o tipo de campo for <b>ip</b> , a lógica pode ser <b>equal</b> ou <b>not_equal</b> . Se o tipo do campo for <b>url</b> , <b>params</b> , <b>cookie</b> , ou <b>header</b> , a lógica pode ser <b>equal</b> , <b>not_equal</b> , <b>contain</b> , <b>not_contain</b> , <b>prefix</b> , <b>not_prefix</b> , <b>suffix</b> , <b>not_suffix</b> .
check_all_indexes_logic	Integer	Este parâmetro é reservado e pode ser ignorado.

Parâmetro	Tipo	Descrição
index	String	Se o tipo de campo for <b>ip</b> e o subcampo for o endereço IP do cliente, o parâmetro <b>index</b> não existirá. Se o tipo de subcampo for <b>X-Forwarded-For</b> , o valor será <b>x-forwarded-for</b> . Se o tipo de campo for <b>params</b> , <b>header</b> , ou <b>cookie</b> , e o subcampo for definido pelo usuário, o valor de <b>index</b> será o subcampo definido pelo usuário.

**Tabela 4-261** Avançado

Parâmetro	Tipo	Descrição
index	String	Tipo de campo. Os seguintes tipos de campo são suportados: Params, Cookie, Header, Body e Multipart. <ul style="list-style-type: none"> <li>● Ao selecionar <b>Params</b>, <b>Cookie</b>, ou <b>Header</b>, você pode definir esse parâmetro para <b>all</b> ou configurar subcampos conforme necessário.</li> <li>● Quando você seleciona <b>Body</b> ou <b>Multipart</b>, defina este parâmetro como <b>all</b>.</li> </ul>
contensts	Array of strings	Subcampo do tipo de campo especificado. O valor padrão é <b>all</b> .

**Código de estado: 400**

**Tabela 4-262** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-263** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro



**Código de estado: 500**

**Tabela 4-264** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Exemplos de solicitações**

```
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"
}
```

**Exemplo de respostas**

**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 status**

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.

Código de status	Descrição
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.4.4 Exclusão de uma regra de lista branca de proteção global (Anteriormente mascaramento de alarme falso)

#### Função

Exclusão de uma regra de lista branca de proteção global (Anteriormente mascaramento de alarme falso)

#### URI

DELETE /v1/{project\_id}/waf/policy/{policy\_id}/ignore/{rule\_id}

**Tabela 4-265** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .
rule_id	Sim	String	ID de uma regra de mascaramento de alarme falso. Você pode obter o ID da regra no campo <b>id</b> no corpo da resposta da API <b>ListIgnoreRule</b> , que é usada para consultar regras de mascaramento de alarme falso.

**Tabela 4-266** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <code>ListEnterpriseProject</code> do EPS.

## Parâmetros de solicitação

**Tabela 4-267** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <code>X-Subject-Token</code> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <code>application/json; charset=utf8</code>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-268** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
policyid	String	ID da política
timestamp	Long	Timestamp a regra foi criada.
description	String	Descrição da regra
status	Integer	Status da regra. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: A regra está desativada.</li> <li>● <b>1</b>: A regra está ativada.</li> </ul>
url	String	O caminho para falsos alarmes de mascaramento. Este parâmetro só está disponível quando <code>mode</code> está definido como <b>0</b> .

Parâmetro	Tipo	Descrição
rule	String	ID da regra incorporada a ser mascarada. Você pode consultar a ID da regra escolhendo <b>Policies &gt; Policy Name &gt; Basic Web Protection &gt; Protection Rules</b> no console do WAF ou na página de detalhes do evento.
mode	Integer	Número da versão. O valor pode ser <b>0</b> ou <b>1</b> . <b>0</b> : indica a versão antiga V1. <b>1</b> indica a nova versão V2. Quando o valor de <b>mode</b> é <b>0</b> , o campo de <b>conditions</b> não existe, mas os campos <b>url</b> e <b>url_logic</b> existem. Quando o valor de <b>mode</b> é <b>1</b> , os campos <b>url</b> e <b>url_logic</b> não existem, mas o campo <b>conditions</b> existe.
url_logic	String	Lógica de correspondência de URL
conditions	Array of <b>Condition</b> objects	Filtro
advanced	Array of <b>Advanced</b> objects	Configurações avançadas
domains	Array of strings	Nome de domínio ou site protegido

Tabela 4-269 Condição

Parâmetro	Tipo	Descrição
category	String	Tipo de campo. O valor pode ser <b>ip</b> , <b>url</b> , <b>params</b> , <b>cookie</b> , ou <b>header</b> .
contents	Array of strings	Conteúdo. O comprimento da matriz deve ser 1. O formato do conteúdo varia de acordo com os tipos de campo. Por exemplo, se o tipo de campo for <b>ip</b> , o valor deverá ser um endereço IP ou intervalo de endereços IP. Se o tipo de campo for <b>url</b> , o valor deve ser um URL no formato padrão. Se o tipo de campo for parâmetros, cookie ou cabeçalho, o formato do conteúdo não é limitado.
logic_operation	String	A lógica de correspondência varia dependendo do tipo de campo. Por exemplo, se o tipo de campo for <b>ip</b> , a lógica pode ser <b>equal</b> ou <b>not_equal</b> . Se o tipo do campo for <b>url</b> , <b>params</b> , <b>cookie</b> , ou <b>header</b> , a lógica pode ser <b>equal</b> , <b>not_equal</b> , <b>contain</b> , <b>not_contain</b> , <b>prefix</b> , <b>not_prefix</b> , <b>suffix</b> , <b>not_suffix</b> .
check_all_indexes_logic	Integer	Este parâmetro é reservado e pode ser ignorado.

Parâmetro	Tipo	Descrição
index	String	Se o tipo de campo for <b>ip</b> e o subcampo for o endereço IP do cliente, o parâmetro <b>index</b> não existirá. Se o tipo de subcampo for <b>X-Forwarded-For</b> , o valor será <b>x-forwarded-for</b> . Se o tipo de campo for <b>params</b> , <b>header</b> , ou <b>cookie</b> , e o subcampo for definido pelo usuário, o valor de <b>index</b> será o subcampo definido pelo usuário.

**Tabela 4-270** Avançado

Parâmetro	Tipo	Descrição
index	String	Tipo de campo. Os seguintes tipos de campo são suportados: Params, Cookie, Header, Body e Multipart. <ul style="list-style-type: none"> <li>● Ao selecionar <b>Params</b>, <b>Cookie</b>, ou <b>Header</b>, você pode definir esse parâmetro para <b>all</b> ou configurar subcampos conforme necessário.</li> <li>● Quando você seleciona <b>Body</b> ou <b>Multipart</b>, defina este parâmetro como <b>all</b>.</li> </ul>
contensts	Array of strings	Subcampo do tipo de campo especificado. O valor padrão é <b>all</b> .

**Código de estado: 400**

**Tabela 4-271** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-272** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-273** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

Solicitação bem-sucedida.

```
{
  "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 status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.4.5 Consulta de lista de regras da lista negra e da lista branca

### Função

Essa API é usada para consultar a lista de regras de lista negra e lista branca.

### URI

GET /v1/{project\_id}/waf/policy/{policy\_id}/whiteblackip

**Tabela 4-274** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-275** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.
page	Não	Integer	Número de página dos dados a serem retornados durante a consulta de paginação. O valor padrão é <b>1</b> , indicando que os dados na primeira página são retornados. Padrão: <b>1</b>
pagesize	Não	Integer	Número de resultados em cada página durante a consulta de paginação. Faixa de valor: <b>1 a 100</b> . O valor padrão é <b>10</b> , indicando que cada página contém 10 resultados. Padrão: <b>10</b>
name	Não	String	Nome da regra da lista branca ou da lista negra

## Parâmetros de solicitação

**Tabela 4-276** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-277** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	Número das regras da lista branca e da lista negra
items	Array of <b>WhiteBlackIpResponseBody</b> objects	Detalhes das regras da lista negra ou da lista branca

**Tabela 4-278** WhiteBlackIpResponseBody

Parâmetro	Tipo	Descrição
id	String	ID da regra
name	String	Nome da regra da lista branca ou da lista negra
policyid	String	ID da política
timestamp	Long	Timestamp (ms) quando a regra foi criada
description	String	Descrição da regra
status	Integer	Status da regra. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: A regra está desativada.</li> <li>● <b>1</b>: A regra está ativada.</li> </ul>
addr	String	Grupo de endereços IP/endereços IP



Parâmetro	Tipo	Descrição
white	Integer	Ação Protetora <ul style="list-style-type: none"> <li>● <b>0</b>: O WAF bloqueia solicitações que atingem a regra.</li> <li>● <b>1</b>: O WAF permite solicitações que batem na regra.</li> <li>● <b>2</b>: O WAF registra apenas solicitações que atingem a regra.</li> </ul>
ip_group	<b>Ip_group</b> object	Grupo de endereços IP

**Tabela 4-279** Ip\_group

Parâmetro	Tipo	Descrição
id	String	ID do grupo de endereços IP
name	String	Nome do grupo de endereços IP
size	Long	Número de endereços IP ou intervalos de endereços IP no grupo de endereços IP

**Código de estado: 400**

**Tabela 4-280** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-281** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-282** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

OK

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

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.4.6 Criação de uma regra de lista negra/lista branca

### Função

Essa API é usada para criar uma regra de lista negra ou lista branca.

## URI

POST /v1/{project\_id}/waf/policy/{policy\_id}/whiteblackip

**Tabela 4-283** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-284** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-285** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-286** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
name	Sim	String	Nome da rue. O valor pode conter no máximo 64 caracteres. Apenas letras, dígitos, hifens (-), sublinhados (_) e pontos (.) são permitidos.
addr	Não	String	Endereço IP ou intervalos de endereços IP na regra de lista negra ou lista branca, por exemplo, 42.123.120.66 ou 42.123.120.0/16.
description	Não	String	Descrição da regra
white	Sim	Integer	Ação Protetora <ul style="list-style-type: none"> <li>● <b>0</b>: O WAF bloqueia solicitações que atingem a regra.</li> <li>● <b>1</b>: O WAF permite solicitações que batem na regra.</li> <li>● <b>2</b>: O WAF registra apenas solicitações que atingem a regra.</li> </ul>
ip_group_id	Não	String	ID do grupo de endereços IP criado. Use este parâmetro ou <b>addr</b> . Para adicionar um grupo de endereços IP, vá para o console do WAF, escolha <b>Objects &gt; Address Groups</b> , e clique em <b>Add Address Group</b> .

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-287** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
name	String	Nome da regra da lista branca ou da lista negra
policyid	String	ID da política
addr	String	Endereço IP ou intervalos de endereços IP na regra de lista negra ou lista branca, por exemplo, 42.123.120.66 ou 42.123.120.0/16.

Parâmetro	Tipo	Descrição
white	Integer	Ação Protetora <ul style="list-style-type: none"> <li>● <b>0</b>: O WAF bloqueia solicitações que atingem a regra.</li> <li>● <b>1</b>: O WAF permite solicitações que batem na regra.</li> <li>● <b>2</b>: O WAF registra apenas solicitações que atingem a regra.</li> </ul>
ip_group	<b>Ip_group</b> object	Grupo de endereços IP
status	Integer	Status da regra. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: A regra está desativada.</li> <li>● <b>1</b>: A regra está ativada.</li> </ul>
description	String	Descrição da regra
timestamp	Long	Hora em que uma regra é criada. O valor é um carimbo de data/hora de 13 dígitos em milissegundos.

**Tabela 4-288** Ip\_group

Parâmetro	Tipo	Descrição
id	String	ID do grupo de endereços IP
name	String	Nome do grupo de endereços IP
size	Long	Número de endereços IP ou intervalos de endereços IP no grupo de endereços IP

**Código de estado: 400**

**Tabela 4-289** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-290** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-291** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

```
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"
}
```

## Exemplo de respostas

**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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.

Código de status	Descrição
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.4.7 Atualização de uma regra de proteção de lista negra ou lista branca

#### Função

Essa API é usada para atualizar as regras de proteção de listas negras e listas brancas. Você pode atualizar endereços IP, intervalos de endereços IP, ações de proteção e outras informações.

#### URI

PUT /v1/{project\_id}/waf/policy/{policy\_id}/whiteblackip/{rule\_id}

**Tabela 4-292** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .
rule_id	Sim	String	ID da regra da lista negra ou da lista branca. Ele pode ser obtido chamando a API <b>**ListWhiteblackipRule</b> .

**Tabela 4-293** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <code>ListEnterpriseProject</code> do EPS.

## Parâmetros de solicitação

**Tabela 4-294** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <code>X-Subject-Token</code> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json; charset=utf8</b>

**Tabela 4-295** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
name	Sim	String	Nome da regra da lista branca ou da lista negra
addr	Não	String	Endereço IP ou intervalos de endereços IP na regra de lista negra ou lista branca, por exemplo, 42.123.120.66 ou 42.123.120.0/16.
description	Não	String	Descrição da regra
white	Sim	Integer	Ação Protetora <ul style="list-style-type: none"> <li>● <b>0</b>: O WAF bloqueia solicitações que atingem a regra.</li> <li>● <b>1</b>: O WAF permite solicitações que batem na regra.</li> <li>● <b>2</b>: O WAF registra apenas solicitações que atingem a regra.</li> </ul>



Parâmetro	Obrigatório	Tipo	Descrição
ip_group_id	Não	String	ID do grupo de endereços IP criado. Use este parâmetro ou <b>addr</b> . Para adicionar um grupo de endereços IP, vá para o console do WAF, escolha <b>Objects &gt; Address Groups</b> , e clique em <b>Add Address Group</b> .

## Parâmetros de resposta

Código de estado: 200

Tabela 4-296 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
name	String	Nome da regra da lista branca ou da lista negra
policyid	String	ID da política
addr	String	Endereço IP ou intervalos de endereços IP incluídos na regra da lista branca ou da lista negra.
description	String	Descrição da regra da lista negra ou da lista branca
white	Integer	Ação Protetora <ul style="list-style-type: none"> <li>● <b>0</b>: O WAF bloqueia solicitações que atingem a regra.</li> <li>● <b>1</b>: O WAF permite solicitações que batem na regra.</li> <li>● <b>2</b>: O WAF registra apenas solicitações que atingem a regra.</li> </ul>
ip_group	<a href="#">Ip_group</a> object	Grupo de endereços IP

Tabela 4-297 Ip\_group

Parâmetro	Tipo	Descrição
id	String	ID do grupo de endereços IP
name	String	Nome do grupo de endereços IP
size	Long	Número de endereços IP ou intervalos de endereços IP no grupo de endereços IP

### Código de estado: 400

Tabela 4-298 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 401

Tabela 4-299 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 500

Tabela 4-300 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

```
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"
}
```

## Exemplo de respostas

### Código de estado: 200

Solicitação bem-sucedida.

```
{
  "id" : "5d43af25404341058d5ab17b7ba78b56",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650531872900,
```

```

"description" : "demo",
"status" : 1,
"addr" : "1.1.1.2",
"white" : 0
}

```

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.4.8 Exclusão de uma regra de lista negra ou de lista branca

#### Função

Essa API é usada para excluir uma regra de lista negra ou de lista branca.

#### URI

DELETE /v1/{project\_id}/waf/policy/{policy\_id}/whiteblackip/{rule\_id}

**Tabela 4-301** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .
rule_id	Sim	String	ID de uma regra de lista negra ou lista branca. Você pode obter o ID da regra chamando a API <b>ListWhiteblackipRule</b> .

**Tabela 4-302** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-303** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-304** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
policyid	String	ID da política
name	String	Nome da regra da lista branca ou da lista negra
timestamp	Long	Hora em que uma regra é excluída. O valor deve ser um carimbo de data/hora de 13 dígitos em milissegundos.
description	String	Descrição
status	Integer	Status da regra. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: A regra está desativada.</li> <li>● <b>1</b>: A regra está ativada.</li> </ul>
addr	String	Endereço IP ou intervalos de endereços IP na regra de lista negra ou lista branca, por exemplo, 42.123.120.66 ou 42.123.120.0/16.

Parâmetro	Tipo	Descrição
white	Integer	Ação Protetora <ul style="list-style-type: none"> <li>● <b>0</b>: O WAF bloqueia solicitações que atingem a regra.</li> <li>● <b>1</b>: O WAF permite solicitações que batem na regra.</li> <li>● <b>2</b>: O WAF registra apenas solicitações que atingem a regra.</li> </ul>
ip_group	<b>Ip_group</b> object	Grupo de endereços IP

**Tabela 4-305** Ip\_group

Parâmetro	Tipo	Descrição
id	String	ID do grupo de endereços IP
name	String	Nome do grupo de endereços IP
size	Long	Número de endereços IP ou intervalos de endereços IP no grupo de endereços IP

**Código de estado: 400**

**Tabela 4-306** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-307** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-308** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

Solicitação bem-sucedida.

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

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.4.9 Consulta de uma regra de mascaramento de dados

### Função

Essa API é usada para consultar uma regra de mascaramento de dados.

## URI

GET /v1/{project\_id}/waf/policy/{policy\_id}/privacy

**Tabela 4-309** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-310** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.
page	Não	Integer	Número de página dos dados a serem retornados durante a consulta de paginação. O valor padrão é <b>1</b> , indicando que os dados na primeira página são retornados.
pagesize	Não	Integer	Número de resultados em cada página durante a consulta de paginação. Faixa de valor: <b>1 a 100</b> . O valor padrão é <b>10</b> , indicando que cada página contém 10 resultados.

## Parâmetros de solicitação

**Tabela 4-311** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).

Parâmetro	Obrigatório	Tipo	Descrição
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json; charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-312** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	Número de regras
items	Array of <b>PrivacyResponseBody</b> objects	Matriz de detalhes da regra

**Tabela 4-313** PrivacyResponseBody

Parâmetro	Tipo	Descrição
id	String	ID da regra
policyid	String	ID da política
timestamp	Long	Hora em que a regra foi criada. O valor é um carimbo de data/hora de 13 dígitos em ms.
status	Integer	Status da regra. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: A regra está desativada.</li> <li>● <b>1</b>: A regra está ativada.</li> </ul>
url	String	URL protegido pela regra de mascaramento de dados. O valor deve estar no formato de URL padrão, por exemplo, /admin/xxx ou /admin/. <i>The asterisk (*)</i> indica o prefixo do caminho.



Parâmetro	Tipo	Descrição
category	String	<p>Campo mascarado.</p> <ul style="list-style-type: none"> <li>● <b>Params</b>: O campo <b>params</b> em solicitações</li> <li>● <b>Cookie</b>: Visitantes da Web distinguidos por cookies</li> <li>● <b>Header</b>: Cabeçalho HTTP personalizado</li> <li>● <b>Form</b>: Formulários</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>params</b></li> <li>● <b>cookie</b></li> <li>● <b>header</b></li> <li>● <b>form</b></li> </ul>
index	String	Nome do campo mascarado. Defina o nome do campo com base no campo mascarado. O campo mascarado não será exibido nos logs.
description	String	(Opcional) Uma descrição da regra.

**Código de estado: 400**

**Tabela 4-314** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-315** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-316** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

Solicitação bem-sucedida.

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

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.4.10 Criação de uma regra de mascaramento de dados

### Função

Essa API é usada para criar uma regra de mascaramento de dados.

## URI

POST /v1/{project\_id}/waf/policy/{policy\_id}/privacy

**Tabela 4-317** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-318** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-319** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-320** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
url	Sim	String	URL protegido pela regra de mascaramento de dados. O valor deve estar no formato de URL padrão, por exemplo, /admin/xxx ou /admin/. <i>The asterisk (*)</i> indica o prefixo do caminho.
category	Sim	String	Campo mascarado. <ul style="list-style-type: none"> <li>● <b>Params:</b> O campo <b>params</b> em solicitações</li> <li>● <b>Cookie:</b> Visitantes da Web distinguidos por cookies</li> <li>● <b>Header:</b> Cabeçalho HTTP personalizado</li> <li>● <b>Form:</b> Formulários</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>params</b></li> <li>● <b>cookie</b></li> <li>● <b>header</b></li> <li>● <b>form</b></li> </ul>
index	Sim	String	Nome do campo mascarado. Defina o nome do campo com base no campo mascarado. O campo mascarado não será exibido nos logs. O nome do campo mascarado não pode exceder bytes de 2 048. Apenas números, letras, sublinhados (_) e hifens (-) são permitidos.
description	Não	String	(Opcional) Uma descrição da regra.

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-321** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
policyid	String	ID da política

Parâmetro	Tipo	Descrição
timestamp	Long	Hora em que a regra foi criada. O valor é um carimbo de data/hora de 13 dígitos em ms.
status	Integer	Status da regra. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: A regra está desativada.</li> <li>● <b>1</b>: A regra está ativada.</li> </ul>
url	String	URL protegido pela regra de mascaramento de dados. O valor deve estar no formato de URL padrão, por exemplo, /admin/xxx ou /admin/. <i>The asterisk ()</i> indica o prefixo do caminho.
category	String	Campo mascarado. <ul style="list-style-type: none"> <li>● <b>Params</b>: O campo <b>params</b> em solicitações</li> <li>● <b>Cookie</b>: Visitantes da Web distinguidos por cookies</li> <li>● <b>Header</b>: Cabeçalho HTTP personalizado</li> <li>● <b>Form</b>: Formulários</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>params</b></li> <li>● <b>cookie</b></li> <li>● <b>header</b></li> <li>● <b>form</b></li> </ul>
index	String	Nome do campo mascarado. Defina o nome do campo com base no campo mascarado. O campo mascarado não será exibido nos logs.
description	String	(Opcional) Uma descrição da regra.

#### Código de estado: 400

**Tabela 4-322** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

#### Código de estado: 401

**Tabela 4-323** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-324** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

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

## Exemplo de respostas

**Código de estado: 200**

Solicitação bem-sucedida.

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

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.

Código de status	Descrição
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.4.11 Atualização de uma regra de mascaramento de dados

#### Função

Essa API é usada para atualizar uma regra de mascaramento de dados.

#### URI

PUT /v1/{project\_id}/waf/policy/{policy\_id}/privacy/{rule\_id}

**Tabela 4-325** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .
rule_id	Sim	String	ID da regra de mascaramento de dados. Você pode obter o ID da regra chamando a API <b>ListPrivacyRule</b> , usada para consultar a lista de regras de mascaramento de dados.

**Tabela 4-326** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-327** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-328** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
url	Sim	String	URL protegido pela regra de mascaramento de dados. O valor deve estar no formato de URL padrão, por exemplo, /admin/xxx ou /admin/. <i>The asterisk (*)</i> indica o prefixo do caminho.
category	Sim	String	Campo mascarado. <ul style="list-style-type: none"> <li>● <b>Params:</b> O campo <b>params</b> em solicitações</li> <li>● <b>Cookie:</b> Visitantes da Web distinguidos por cookies</li> <li>● <b>Header:</b> Cabeçalho HTTP personalizado</li> <li>● <b>Form:</b> Formulários</li> </ul> Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>params</b></li> <li>● <b>cookie</b></li> <li>● <b>header</b></li> <li>● <b>form</b></li> </ul>



Parâmetro	Obrigatório	Tipo	Descrição
index	Sim	String	Nome do campo mascarado. Defina o nome do campo com base no campo mascarado. O campo mascarado não será exibido nos logs. O nome do campo mascarado não pode exceder bytes de 2 048. Apenas números, letras, sublinhados ( _ ) e hifens ( - ) são permitidos.
description	Não	String	(Opcional) Uma descrição da regra.

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-329** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
policyid	String	ID da política
timestamp	Long	Hora em que a regra foi criada. O valor é um carimbo de data/hora de 13 dígitos em ms.
status	Integer	Status da regra. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: A regra está desativada.</li> <li>● <b>1</b>: A regra está ativada.</li> </ul>
url	String	URL protegido pela regra de mascaramento de dados. O valor deve estar no formato de URL padrão, por exemplo, /admin/xxx ou /admin/. <i>The asterisk ( )</i> indica o prefixo do caminho.

Parâmetro	Tipo	Descrição
category	String	<p>Campo mascarado.</p> <ul style="list-style-type: none"> <li>● <b>Params</b>: O campo <b>params</b> em solicitações</li> <li>● <b>Cookie</b>: Visitantes da Web distinguidos por cookies</li> <li>● <b>Header</b>: Cabeçalho HTTP personalizado</li> <li>● <b>Form</b>: Formulários</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>params</b></li> <li>● <b>cookie</b></li> <li>● <b>header</b></li> <li>● <b>form</b></li> </ul>
index	String	Nome do campo mascarado. Defina o nome do campo com base no campo mascarado. O campo mascarado não será exibido nos logs.
description	String	(Opcional) Uma descrição da regra.

**Código de estado: 400**

**Tabela 4-330** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-331** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-332** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

```
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"
}
```

## Exemplo de respostas

**Código de estado: 200**

Solicitação bem-sucedida.

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

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.4.12 Exclusão de uma regra de mascaramento de dados

### Função

Essa API é usada para excluir uma regra de mascaramento de dados.

### URI

DELETE /v1/{project\_id}/waf/policy/{policy\_id}/privacy/{rule\_id}

**Tabela 4-333** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .
rule_id	Sim	String	ID da regra de mascaramento de dados. Você pode obter o ID da regra chamando a API <b>ListPrivacyRule</b> , usada para consultar a lista de regras de mascaramento de dados.

**Tabela 4-334** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

Tabela 4-335 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

Código de estado: 200

Tabela 4-336 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
policyid	String	ID da política
timestamp	Long	Hora em que a regra foi criada. O valor é um carimbo de data/hora de 13 dígitos em ms.
description	String	(Opcional) Uma descrição da regra.
status	Integer	Status da regra. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: A regra está desativada.</li> <li>● <b>1</b>: A regra está ativada.</li> </ul>
url	String	URL protegido pela regra de mascaramento de dados. O valor deve estar no formato de URL padrão, por exemplo, /admin/xxx ou /admin/. <i>The asterisk (*)</i> indica o prefixo do caminho.
category	String	Campo mascarado. <ul style="list-style-type: none"> <li>● <b>Params</b>: O campo <b>params</b> em solicitações</li> <li>● <b>Cookie</b>: Visitantes da Web distinguidos por cookies</li> <li>● <b>Header</b>: Cabeçalho HTTP personalizado</li> <li>● <b>Form</b>: Formulários</li> </ul>
index	String	Nome do campo mascarado. Defina o nome do campo com base no campo mascarado. O campo mascarado não será exibido nos logs.

### Código de estado: 400

**Tabela 4-337** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 401

**Tabela 4-338** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 500

**Tabela 4-339** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

### Código de estado: 200

Solicitação bem-sucedida.

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

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.4.13 Consulta de lista de regras de controle de acesso de geolocalização

#### Função

Consulta de lista de regras de controle de acesso de geolocalização

#### URI

GET /v1/{project\_id}/waf/policy/{policy\_id}/geoip

**Tabela 4-340** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-341** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.
page	Não	Integer	Número de página dos dados a serem retornados durante a consulta de paginação. O valor padrão é <b>1</b> , indicando que os dados na primeira página são retornados. Padrão: <b>1</b>
pagesize	Não	Integer	Número de resultados em cada página durante a consulta de paginação. Faixa de valor: <b>1 a 100</b> . O valor padrão é <b>10</b> , indicando que cada página contém 10 resultados. Padrão: <b>10</b>

## Parâmetros de solicitação

**Tabela 4-342** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-343** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	Número de regras de controle de acesso de geolocalização na política



Parâmetro	Tipo	Descrição
items	Array of <b>GeoIpItem</b> objects	Matriz de geolocalização controle de acesso rues

Tabela 4-344 GeoIpItem

Parâmetro	Tipo	Descrição
id	String	ID da regra
policyid	String	ID da política
name	String	Nome da rua de controle de acesso de geolocalização
geoip	String	Locais que podem ser configurados na regra de controle de acesso de geolocalização: <b>(CN: China, CA: Canadá, US: Estados Unidos, AU: Austrália, IN: Índia, JP: Japão, UK: Reino Unido, FR: França, DE: Alemanha, BR: Brasil, Ukraine: Ucrânia, North Korea: Coreia do Norte, The Republic of Korea: Coreia do Sul, Iran: Irã, Cuba: Cuba, Sultan: Sudão, Syria: Síria, Pakistan: Paquistão, Palestine: Palestina, Israel: Israel, Iraq: Iraque, Afghanistan: Afeganistão, Libya: Líbia, Turkey: Turquia, Thailand: Tailândia, Singapore: Singapura, South Africa: México, South Africa: México, Peru: Peru, Indonesia: Indonésia, GD Guangdong, FJ: Fujian, JL: Jilin, LN: Liaoning, TW: Taiwan, GZ: Guizhou, AH: Anhui, HL: Heilongjiang, HA: Henan, SC: Sichuan, HE: Em Hebei, YN: Yunnan, HB: Hubei, HI: Hainão, QH: Qinghai, HN: Hunan, JX: Jiangxi, SX: Shanxi, SN: Shaanxi, ZJ: Zhejiang, GS: Gansu, JS: Jiangsu, SD: Shandong, BJ: Pequim, SH: Xangai, TJ: Tianjin, CQ: Chongqing, MO: Macau (China), HK: Hong Kong (China), NX: Ningxia, GX: Guangxi, XJ: Xinjiang, XZ: Tibete, NM: Mongólia Interior</b>
white	Integer	Ação Protetora <ul style="list-style-type: none"> <li>● <b>0</b>: O WAF bloqueia solicitações que atingem a regra.</li> <li>● <b>1</b>: O WAF permite solicitações que batem na regra.</li> <li>● <b>2</b>: O WAF registra apenas solicitações que atingem a regra.</li> </ul>
status	Integer	Status da regra. <ul style="list-style-type: none"> <li>● <b>true</b>: ativado.</li> <li>● <b>false</b>: desativado.</li> </ul>

Parâmetro	Tipo	Descrição
timestamp	Long	Hora em que a regra é criada.

**Código de estado: 400**

**Tabela 4-345** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-346** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-347** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "06f07f6c229141b9a4a78614751bb687",
```

```

    "policyid" : "2abeecefb9840e6bf05efbd80d0fcd7",
    "timestamp" : 1636340038062,
    "status" : 1,
    "geoip" : "GD",
    "white" : 1,
    "name" : "demo"
  } ]
}

```

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.4.14 Atualização de uma regra de controle de acesso de geolocalização

#### Função

Atualização de uma regra de controle de acesso de geolocalização

#### URI

POST /v1/{project\_id}/waf/policy/{policy\_id}/geoip

**Tabela 4-348** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-349** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-350** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json; charset=utf8</b>

**Tabela 4-351** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
name	Não	String	Nome da rua de controle de acesso de geolocalização

Parâmetro	Obrigatório	Tipo	Descrição
geoip	Sim	String	Locais geográficos que podem ser usados para controle de acesso. Use um ( ) de barra vertical para separar cada dois códigos de localização. (CN: China, CA: Canadá, US: Estados Unidos, AU: Austrália, IN: Índia, JP: Japão, UK: Reino Unido, FR: França, DE: Alemanha, BR: Brasil, Ukraine: Ucrânia, North Korea: Coreia do Norte, The Republic of Korea: Coreia do Sul, Iran: Irã, Cuba: Cuba, Sultan: Sudão, Syria: Síria, Pakistan: Paquistão, Palestine Palestina, Israel Israel, Iraq: Iraque, Afghanistan: Afeganistão, Libya: Líbia, Turkey: Turquia, Thailand: Tailândia, Singapore: Singapura, South Africa: México, South Africa: México, Peru: Peru, Indonesia: Indonésia, GD Guangdong, FJ: Fujian, JL: Jilin, LN: Liaoning, TW: Taiwan, GZ: Guizhou, AH: Anhui, HL: Heilongjiang, HA: Henan, SC: Sichuan, HE: Em Hebei, YN: Yunnan, HB: Hubei, HI: Hainão, QH: Qinghai, HN: Hunan, JX: Jiangxi, SX: Shanxi, SN: Shaanxi, ZJ: Zhejiang, GS: Gansu, JS: Jiangsu, SD: Shandong, BJ: Pequim, SH: Xangai, TJ: Tianjin, CQ: Chongqing, MO: Macau (China), HK: Hong Kong (China), NX: Ningxia, GX: Guangxi, XJ: Xinjiang, XZ: Tibete, NM: Mongólia Interior
white	Sim	Integer	Ação Protetora <ul style="list-style-type: none"> <li>● <b>0</b>: O WAF bloqueia solicitações que atingem a regra.</li> <li>● <b>1</b>: O WAF permite solicitações que batem na regra.</li> <li>● <b>2</b>: O WAF registra apenas solicitações que atingem a regra.</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
status	Não	Integer	Status da regra. <ul style="list-style-type: none"> <li>● <b>true</b>: ativado.</li> <li>● <b>false</b>: desativado.</li> </ul>
description	Não	String	Descrição da regra

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-352** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
name	String	Nome da rua de controle de acesso de geolocalização
policyid	String	ID da política
geoip	String	Locais que podem ser configurados na regra de controle de acesso de geolocalização: <b>CN</b> : China <b>CA</b> : Canadá, <b>US</b> : Estados Unidos, <b>AU</b> : Austrália, <b>IN</b> : Índia, <b>JP</b> : Japão, <b>UK</b> : Reino Unido, <b>FR</b> : França, <b>DE</b> : Alemanha, <b>BR</b> : Brasil, <b>Ukraine</b> : Ucrânia, <b>North Korea</b> : Coreia do Norte, <b>The Republic of Korea</b> : Coreia do Sul, <b>Iran</b> : Irã, <b>Cuba</b> : Cuba, <b>Sultan</b> : Sudão, <b>Syria</b> : Síria, <b>Pakistan</b> : Paquistão, <b>Palestine</b> Palestina, <b>Israel</b> Israel, <b>Iraq</b> : Iraque, <b>Afghanistan</b> : Afeganistão, <b>Libya</b> : Líbia, <b>Turkey</b> : Turquia, <b>Thailand</b> : Tailândia, <b>Singapore</b> : Singapura, <b>South Africa</b> : México, <b>South Africa</b> : México, <b>Peru</b> : Peru, <b>Indonesia</b> : Indonésia, <b>GD</b> Guangdong, <b>FJ</b> : Fujian, <b>JL</b> : Jilin, <b>LN</b> : Liaoning, <b>TW</b> : Taiwan, <b>GZ</b> : Guizhou, <b>AH</b> : Anhui, <b>HL</b> : Heilongjiang, <b>HA</b> : Henan, <b>SC</b> : Sichuan, <b>HE</b> : Em Hebei, <b>YN</b> : Yunnan, <b>HB</b> : Hubei, <b>HI</b> : Hainão, <b>QH</b> : Qinghai, <b>HN</b> : Hunan, <b>JX</b> : Jiangxi, <b>SX</b> : Shanxi, <b>SN</b> : Shaanxi, <b>ZJ</b> : Zhejiang, <b>GS</b> : Gansu, <b>JS</b> : Jiangsu, <b>SD</b> : Shandong, <b>BJ</b> : Pequim, <b>SH</b> : Xangai, <b>TJ</b> : Tianjin, <b>CQ</b> : Chongqing, <b>MO</b> : Macau (China), <b>HK</b> : Hong Kong (China), <b>NX</b> : Ningxia, <b>GX</b> : Guangxi, <b>XJ</b> : Xinjiang, <b>XZ</b> : Tibete, <b>NM</b> : Mongólia Interior

Parâmetro	Tipo	Descrição
white	Integer	Ação Protetora <ul style="list-style-type: none"> <li>● <b>0</b>: O WAF bloqueia solicitações que atingem a regra.</li> <li>● <b>1</b>: O WAF permite solicitações que batem na regra.</li> <li>● <b>2</b>: O WAF registra apenas solicitações que atingem a regra.</li> </ul>
status	Integer	Status da regra. <ul style="list-style-type: none"> <li>● <b>true</b>: ativado.</li> <li>● <b>false</b>: desativado.</li> </ul>
timestamp	Long	Hora em que a regra é criada.

**Código de estado: 400**

**Tabela 4-353** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-354** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-355** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

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

## Exemplo de respostas

**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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.4.15 Atualização de uma regra de controle de acesso de geolocalização

#### Função

Atualização de uma regra de controle de acesso de geolocalização

#### URI

PUT /v1/{project\_id}/waf/policy/{policy\_id}/geoip/{rule\_id}



**Tabela 4-356** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> (valor do campo <b>id</b> no corpo da resposta).
rule_id	Sim	String	ID da regra de controle de acesso de geolocalização. Você pode obter o ID da regra chamando a API <b>ListGeoipRule</b> , usada para consultar a lista de regras de controle de acesso de geolocalização. A ID da regra é incluída no campo <b>id</b> no corpo da resposta.

**Tabela 4-357** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-358** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-359** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
name	Não	String	Nome da rua de controle de acesso de geolocalização
description	Não	String	descrição
geoip	Sim	String	Locais que podem ser configurados na regra de controle de acesso de geolocalização: ( <b>CN</b> : China <b>CA</b> : Canadá, <b>US</b> : Estados Unidos, <b>AU</b> : Austrália, <b>IN</b> : Índia, <b>JP</b> : Japão, <b>UK</b> : Reino Unido, <b>FR</b> : França, <b>DE</b> : Alemanha, <b>BR</b> : Brasil, <b>Ukraine</b> : Ucrânia, <b>North Korea</b> : Coreia do Norte, <b>The Republic of Korea</b> : Coreia do Sul, <b>Iran</b> : Irã, <b>Cuba</b> : Cuba, <b>Sultan</b> : Sudão, <b>Syria</b> : Síria, <b>Pakistan</b> : Paquistão, <b>Palestine</b> : Palestina, <b>Israel</b> : Israel, <b>Iraq</b> : Iraque, <b>Afghanistan</b> : Afeganistão, <b>Libya</b> : Líbia, <b>Turkey</b> : Turquia, <b>Thailand</b> : Tailândia, <b>Singapore</b> : Singapura, <b>South Africa</b> : México, <b>South Africa</b> : México, <b>Peru</b> : Peru, <b>Indonesia</b> : Indonésia, <b>GD</b> : Guangdong, <b>FJ</b> : Fujian, <b>JL</b> : Jilin, <b>LN</b> : Liaoning, <b>TW</b> : Taiwan, <b>GZ</b> : Guizhou, <b>AH</b> : Anhui, <b>HL</b> : Heilongjiang, <b>HA</b> : Henan, <b>SC</b> : Sichuan, <b>HE</b> : Em Hebei, <b>YN</b> : Yunnan, <b>HB</b> : Hubei, <b>HI</b> : Hainão, <b>QH</b> : Qinghai, <b>HN</b> : Hunan, <b>JX</b> : Jiangxi, <b>SX</b> : Shanxi, <b>SN</b> : Shaanxi, <b>ZJ</b> : Zhejiang, <b>GS</b> : Gansu, <b>JS</b> : Jiangsu, <b>SD</b> : Shandong, <b>BJ</b> : Pequim, <b>SH</b> : Xangai, <b>TJ</b> : Tianjin, <b>CQ</b> : Chongqing, <b>MO</b> : Macau (China), <b>HK</b> : Hong Kong (China), <b>NX</b> : Ningxia, <b>GX</b> : Guangxi, <b>XJ</b> : Xinjiang, <b>XZ</b> : Tibete, <b>NM</b> : Mongólia Interior

Parâmetro	Obrigatório	Tipo	Descrição
white	Sim	Integer	Ação Protetora <ul style="list-style-type: none"> <li>● <b>0</b>: O WAF bloqueia solicitações que atingem a regra.</li> <li>● <b>1</b>: O WAF permite solicitações que batem na regra.</li> <li>● <b>2</b>: O WAF registra apenas solicitações que atingem a regra.</li> </ul>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-360** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
name	String	Nome da rua de controle de acesso de geolocalização
description	String	Descrição
policyid	String	ID da política
geoip	String	Locais que podem ser configurados na regra de controle de acesso de geolocalização: <b>CN</b> : China <b>CA</b> : Canadá, <b>US</b> : Estados Unidos, <b>AU</b> : Austrália, <b>IN</b> : Índia, <b>JP</b> : Japão, <b>UK</b> : Reino Unido, <b>FR</b> : França, <b>DE</b> : Alemanha, <b>BR</b> : Brasil, <b>Ukraine</b> : Ucrânia, <b>North Korea</b> : Coreia do Norte, <b>The Republic of Korea</b> : Coreia do Sul, <b>Iran</b> : Irã, <b>Cuba</b> : Cuba, <b>Sultan</b> : Sudão, <b>Syria</b> : Síria, <b>Pakistan</b> : Paquistão, <b>Palestine</b> Palestina, <b>Israel</b> Israel, <b>Iraq</b> : Iraque, <b>Afghanistan</b> : Afeganistão, <b>Libya</b> : Líbia, <b>Turkey</b> : Turquia, <b>Thailand</b> : Tailândia, <b>Singapore</b> : Singapura, <b>South Africa</b> : México, <b>South Africa</b> : México, <b>Peru</b> : Peru, <b>Indonesia</b> : Indonésia, <b>GD</b> Guangdong, <b>FJ</b> : Fujian, <b>JL</b> : Jilin, <b>LN</b> : Liaoning, <b>TW</b> : Taiwan, <b>GZ</b> : Guizhou, <b>AH</b> : Anhui, <b>HL</b> : Heilongjiang, <b>HA</b> : Henan, <b>SC</b> : Sichuan, <b>HE</b> : Em Hebei, <b>YN</b> : Yunnan, <b>HB</b> : Hubei, <b>HI</b> : Hainão, <b>QH</b> : Qinghai, <b>HN</b> : Hunan, <b>JX</b> : Jiangxi, <b>SX</b> : Shanxi, <b>SN</b> : Shaanxi, <b>ZJ</b> : Zhejiang, <b>GS</b> : Gansu, <b>JS</b> : Jiangsu, <b>SD</b> : Shandong, <b>BJ</b> : Pequim, <b>SH</b> : Xangai, <b>TJ</b> : Tianjin, <b>CQ</b> : Chongqing, <b>MO</b> : Macau (China), <b>HK</b> : Hong Kong (China), <b>NX</b> : Ningxia, <b>GX</b> : Guangxi, <b>XJ</b> : Xinjiang, <b>XZ</b> : Tibete, <b>NM</b> : Mongólia Interior

Parâmetro	Tipo	Descrição
white	número inteiro	Ação protetora <ul style="list-style-type: none"> <li>● <b>0</b>: O WAF bloqueia solicitações que atingem a regra.</li> <li>● <b>1</b>: O WAF permite solicitações que batem na regra.</li> <li>● <b>2</b>: O WAF registra apenas solicitações que atingem a regra.</li> </ul>

#### Código de estado: 400

**Tabela 4-361** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

#### Código de estado: 401

**Tabela 4-362** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

#### Código de estado: 500

**Tabela 4-363** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

{
  "white" : 0,
```

```
"name" : "demo",  
"geoip" : "BJ|Afghanistan"  
}
```

## Exemplo de respostas

**Código de estado: 200**

Solicitação bem-sucedida.

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

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.4.16 Exclusão de uma regra de controle de acesso de geolocalização

#### Função

Essa API é usada para excluir uma regra de controle de acesso de geolocalização.

#### URI

DELETE /v1/{project\_id}/waf/policy/{policy\_id}/geoip/{rule\_id}

**Tabela 4-364** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .
rule_id	Sim	String	ID da regra de controle de acesso de geolocalização. Você pode obter o ID da regra chamando a API <b>ListGeoipRule</b> , usada para consultar a lista de regras de controle de acesso de geolocalização. A ID da regra é incluída no campo <b>id</b> no corpo da resposta.

**Tabela 4-365** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-366** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-367** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
name	String	Nome da rua de controle de acesso de geolocalização
policyid	String	ID da política
geoip	String	Locais que podem ser configurados na regra de controle de acesso de geolocalização: <b>CN</b> : China, <b>CA</b> : Canadá, <b>US</b> : Estados Unidos, <b>AU</b> : Austrália, <b>IN</b> : Índia, <b>JP</b> : Japão, <b>UK</b> : Reino Unido, <b>FR</b> : França, <b>DE</b> : Alemanha, <b>BR</b> : Brasil, <b>Ukraine</b> : Ucrânia, <b>North Korea</b> : Coreia do Norte, <b>The Republic of Korea</b> : Coreia do Sul, <b>Iran</b> : Irã, <b>Cuba</b> : Cuba, <b>Sultan</b> : Sudão, <b>Syria</b> : Síria, <b>Pakistan</b> : Paquistão, <b>Palestine</b> : Palestina, <b>Israel</b> : Israel, <b>Iraq</b> : Iraque, <b>Afghanistan</b> : Afeganistão, <b>Libya</b> : Líbia, <b>Turkey</b> : Turquia, <b>Thailand</b> : Tailândia, <b>Singapore</b> : Singapura, <b>South Africa</b> : África do Sul, <b>South Africa</b> : México, <b>Peru</b> : Peru, <b>Indonesia</b> : Indonésia, <b>GD</b> : Guangdong, <b>FJ</b> : Fujian, <b>JL</b> : Jilin, <b>LN</b> : Liaoning, <b>TW</b> : Taiwan, <b>GZ</b> : Guizhou, <b>AH</b> : Anhui, <b>HL</b> : Heilongjiang, <b>HA</b> : Henan, <b>SC</b> : Sichuan, <b>HE</b> : Hebei, <b>YN</b> : Yunnan, <b>HB</b> : Hubei, <b>HI</b> : Hainan, <b>QH</b> : Qinghai, <b>HN</b> : Hunan, <b>JX</b> : Jiangxi, <b>SX</b> : Shanxi, <b>SN</b> : Shaanxi, <b>ZJ</b> : Zhejiang, <b>GS</b> : Gansu, <b>JS</b> : Jiangsu, <b>SD</b> : Shandong, <b>BJ</b> : Pequim, <b>SH</b> : Xangai, <b>TJ</b> : Tianjin, <b>CQ</b> : Chongqing, <b>MO</b> : Macau (China), <b>HK</b> : Hong Kong (China), <b>NX</b> : Ningxia, <b>GX</b> : Guangxi, <b>XJ</b> : Xinjiang, <b>XZ</b> : Tibete, <b>NM</b> : Mongólia Interior
white	Integer	Ação Protetora <ul style="list-style-type: none"> <li>● <b>0</b>: O WAF bloqueia solicitações que atingem a regra.</li> <li>● <b>1</b>: O WAF permite solicitações que batem na regra.</li> <li>● <b>2</b>: O WAF registra apenas solicitações que atingem a regra.</li> </ul>
status	Integer	Status da regra. <ul style="list-style-type: none"> <li>● <b>true</b>: ativado.</li> <li>● <b>false</b>: desativado.</li> </ul>
description	String	Descrição
timestamp	Long	Hora em que a regra é criada.

### Código de estado: 400

**Tabela 4-368** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 401

**Tabela 4-369** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 500

**Tabela 4-370** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

### Código de estado: 200

Solicitação bem-sucedida.

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



## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.4.17 Consulta de lista de regras de proteção contra intrusão na Web

#### Função

Essa API é usada para consultar a lista de regras de proteção contra adulteração da Web.

#### URI

GET /v1/{project\_id}/waf/policy/{policy\_id}/antitamper

**Tabela 4-371** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-372** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.
page	Não	Integer	Número de página dos dados a serem retornados durante a consulta de paginação. O valor padrão é <b>1</b> , indicando que os dados na primeira página são retornados.
pagesize	Não	Integer	Número de resultados em cada página durante a consulta de paginação. Faixa de valor: <b>1 a 100</b> . O valor padrão é <b>10</b> , indicando que cada página contém 10 resultados.

## Parâmetros de solicitação

**Tabela 4-373** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json; charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-374** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	Número total de regras de proteção contra adulteração da web
items	Array of <b>AntiTamperRuleResponseBody</b> objects	Número de regras de proteção contra violação da web.

**Tabela 4-375** AntiTamperRuleResponseBody

Parâmetro	Tipo	Descrição
id	String	ID da regra
policyid	String	ID da política de proteção que inclui a regra
timestamp	Long	Timestamp a regra foi criada.
description	String	Observações de regra
status	Integer	Status da regra. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: A regra está desativada.</li> <li>● <b>1</b>: A regra está ativada.</li> </ul>
hostname	String	Nome de domínio protegido pela regra de proteção contra adulteração da Web
url	String	URL protegida pela regra de proteção contra adulteração da Web

**Código de estado: 400**

**Tabela 4-376** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-377** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-378** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro

Parâmetro	Tipo	Descrição
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

OK

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

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.4.18 Criação de uma regra de proteção contra violação da Web

#### Função

Essa API é usada para criar uma regra de proteção contra adulteração da Web.

#### URI

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

**Tabela 4-379** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .

**Tabela 4-380** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-381** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-382** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
hostname	Sim	String	Sites protegidos. A lista pode ser obtida chamando a API do <b>ListHost</b> no modo nuvem. (o valor do campo <b>hostname</b> no corpo da resposta).

Parâmetro	Obrigatório	Tipo	Descrição
url	Sim	String	URL protegido pela regra de proteção contra adulteração da Web. O valor deve estar no formato de URL padrão, por exemplo, /admin/xxx ou /admin/. <i>The asterisk ()</i> indica o prefixo do caminho.
description	Não	String	Descrição da regra

## Parâmetros de resposta

### Código de estado: 200

Tabela 4-383 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
policyid	String	ID da política
hostname	String	Nome de domínio protegido pela regra de proteção contra adulteração da Web
url	String	URL protegida pela regra de proteção contra adulteração da Web
description	String	Timestamp a regra foi criada.
status	Integer	Status da regra. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: A regra está desativada.</li> <li>● <b>1</b>: A regra está ativada.</li> </ul>

### Código de estado: 400

Tabela 4-384 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 401

**Tabela 4-385** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-386** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

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

## Exemplo de respostas

**Código de estado: 200**

Solicitação bem-sucedida.

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

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.

Código de status	Descrição
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.4.19 Exclusão de uma regra de proteção contra violação da Web

#### Função

Essa API é usada para excluir uma regra de proteção contra violação da Web.

#### URI

DELETE /v1/{project\_id}/waf/policy/{policy\_id}/antitamper/{rule\_id}

**Tabela 4-387** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
policy_id	Sim	String	ID da política. Ele pode ser obtido chamando a API <b>ListPolicy</b> .
rule_id	Sim	String	ID da regra anti-adulteração. Ele pode ser obtido chamando a API <b>ListAntitamperRule</b> .

**Tabela 4-388** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.



## Parâmetros de solicitação

**Tabela 4-389** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-390** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da regra
policyid	String	ID da política
url	String	URL protegida pela regra de proteção contra adulteração da Web
timestamp	Long	Timestamp a regra foi criada.

**Código de estado: 400**

**Tabela 4-391** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-392** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-393** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

Solicitação bem-sucedida.

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

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.4.20 Consulta de lista de tabelas de referência

#### Função

Essa API é usada para consultar a lista de tabelas de referência.

#### URI

GET /v1/{project\_id}/waf/valuelist

**Tabela 4-394** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

**Tabela 4-395** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
page	Não	Integer	Número de página dos dados a serem retornados durante a consulta de paginação. O valor padrão é <b>1</b> , indicando que os dados na primeira página são retornados.
pagesize	Não	Integer	Número de resultados em cada página durante a consulta de paginação. Faixa de valor: <b>1</b> a <b>100</b> . O valor padrão é <b>10</b> , indicando que cada página contém 10 resultados.
name	Não	String	Nome da tabela de referência

## Parâmetros de solicitação

**Tabela 4-396** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-397** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	Número de tabelas de referência Mínimo: <b>0</b> Máximo: <b>500</b>
items	Array of <b>ValueListResponseBody</b> objects	lista de tabelas de referência

**Tabela 4-398** ValueListResponseBody

Parâmetro	Tipo	Descrição
id	String	ID da tabela de referência
name	String	Nome da tabela de referência.

Parâmetro	Tipo	Descrição
type	String	Tipo de tabela de referência Valores de enumeração: <ul style="list-style-type: none"> <li>● url</li> <li>● params</li> <li>● ip</li> <li>● cookie</li> <li>● referer</li> <li>● user-agent</li> <li>● header</li> <li>● response_code</li> <li>● response_header</li> <li>● response_body</li> </ul>
timestamp	Long	Tabela de referência timestamp
values	Array of strings	Valor da tabela de referência
producer	Integer	Fonte da tabela de referência. O valor pode ser 1 ou outros. 1: A tabela é criada por você. Outros valores indicam que a tabela é gerada automaticamente pelo moduleX.
description	String	Descrição da tabela de referência

**Código de estado: 400**

**Tabela 4-399** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-400** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 500

Tabela 4-401 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

### Código de estado: 200

Solicitação bem-sucedida.

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

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.4.21 Criação de uma tabela de referência

### Função

Essa API é usada para adicionar uma tabela de referência. Uma tabela de referência pode ser usada por regras de proteção de ataque CC e regras de proteção precisas.

### URI

POST /v1/{project\_id}/waf/valuelist

Tabela 4-402 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

Tabela 4-403 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

### Parâmetros de solicitação

Tabela 4-404 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-405** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
name	Sim	String	Nome da tabela de referência. O valor pode conter no máximo 64 caracteres. Somente dígitos, letras, hífen, (_), de sublinhados e pontos (.) são permitidos. Mínimo: <b>2</b> Máximo: <b>64</b>
type	Sim	String	Tipo de tabela de referência. Para obter detalhes, consulte a lista de enumeração. Mínimo: <b>2</b> Máximo: <b>32</b> Valores de enumeração: <ul style="list-style-type: none"> <li>● url</li> <li>● params</li> <li>● ip</li> <li>● cookie</li> <li>● referer</li> <li>● user-agent</li> <li>● header</li> <li>● response_code</li> <li>● response_header</li> <li>● response_body</li> </ul>
values	Sim	Array of strings	Valor da tabela de referência
description	Não	String	Descrição da tabela de referência. O valor contém no máximo 128 caracteres. Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-406** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da tabela de referência



Parâmetro	Tipo	Descrição
name	String	Nome da tabela de referência.
type	String	Tipo de tabela de referência
description	String	Descrição da tabela de referência
timestamp	Long	Tabela de referência timestamp
values	Array of strings	Valor da tabela de referência
producer	Integer	Fonte da tabela de referência. <ul style="list-style-type: none"> <li>● 1: A tabela de referência foi criada por você.</li> <li>● 2: A tabela de referência foi criada pela proteção inteligente de controle de acesso.</li> </ul>

**Código de estado: 400**

**Tabela 4-407** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-408** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-409** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

Solicitação bem-sucedida.

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

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.4.22 Modificação de uma tabela de referência

### Função

Essa API é usada para modificar uma tabela de referência.

### URI

PUT /v1/{project\_id}/waf/valuelist/{valuelistid}

**Tabela 4-410** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
valuelistid	Sim	String	ID da tabela de referência. Ele pode ser obtido chamando a API <b>ListValueList</b> .

**Tabela 4-411** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-412** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-413** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
name	Sim	String	Nome da tabela de referência, que é uma cadeia de 2 a 32 caracteres. Mínimo: <b>2</b> Máximo: <b>32</b>
type	Sim	String	Tipo de tabela de referência. Para obter detalhes, consulte a lista de enumeração. Mínimo: <b>2</b> Máximo: <b>32</b> Valores de enumeração: <ul style="list-style-type: none"> <li>● url</li> <li>● params</li> <li>● ip</li> <li>● cookie</li> <li>● referer</li> <li>● user-agent</li> <li>● header</li> <li>● response_code</li> <li>● response_header</li> <li>● resopnse_body</li> </ul>
values	Não	Array of strings	Valor da tabela de referência
description	Não	String	Descrição da tabela de referência. O valor contém no máximo 128 caracteres. Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-414** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID da tabela de referência
name	String	Nome da tabela de referência.
type	String	Tipo de tabela de referência

Parâmetro	Tipo	Descrição
description	String	Descrição da tabela de referência
values	Array of strings	Valor da tabela de referência
producer	Integer	Fonte da tabela de referência. <ul style="list-style-type: none"> <li>● 1: A tabela de referência foi criada por você.</li> <li>● 2: A tabela de referência foi criada pela proteção inteligente de controle de acesso.</li> </ul>

#### Código de estado: 400

Tabela 4-415 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

#### Código de estado: 401

Tabela 4-416 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

#### Código de estado: 500

Tabela 4-417 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

{
  "name" : "RPmvp0m4",
```

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

## Exemplo de respostas

### Código de estado: 200

Solicitação bem-sucedida.

```
{  
  "id" : "63b1d9edf2594743bc7c6ee98527306c",  
  "name" : "RPMvp0m4",  
  "type" : "response_code",  
  "values" : [ "500" ],  
  "description" : "demo",  
  "producer" : 1  
}
```

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.4.23 Exclusão de uma tabela de referência

### Função

Essa API é usada para excluir uma tabela de referência.

### URI

DELETE /v1/{project\_id}/waf/valuelist/{valuelistid}

**Tabela 4-418** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
valuelistid	Sim	String	ID da tabela de referência. Ele pode ser obtido chamando a API <b>ListValueList</b> .

**Tabela 4-419** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-420** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

Código de estado: 200

**Tabela 4-421** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID de uma tabela de referência
name	String	Nome da tabela de referência.
type	String	Tipo de tabela de referência
timestamp	Long	Hora em que a tabela de referência é eliminada. O valor é um carimbo de data/hora de 13 dígitos em milissegundos.

**Código de estado: 400**

**Tabela 4-422** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-423** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-424** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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



## Exemplo de respostas

### Código de estado: 200

Solicitação bem-sucedida.

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

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

# 4.5 Gerenciamento de certificado

## 4.5.1 Consulta de lista de certificados

### Função

Esta API é usada para consultar a lista de certificados.

### URI

GET /v1/{project\_id}/waf/certificate

**Tabela 4-425** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

**Tabela 4-426** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.
page	Não	Integer	Número de página dos dados a serem retornados durante a consulta de paginação. O valor padrão é <b>1</b> , indicando que os dados na primeira página são retornados. Padrão: <b>1</b>
pagesize	Não	Integer	Número de resultados em cada página durante a consulta de paginação. Faixa de valor: <b>1 a 100</b> . O valor padrão é <b>10</b> , indicando que cada página contém 10 resultados. Padrão: <b>10</b>
name	Não	String	Nome do certificado
host	Não	Boolean	Se deseja obter o nome de domínio para o qual o certificado é usado. O valor padrão é <b>false</b> . <ul style="list-style-type: none"> <li>● <b>true</b>: Obtenha os certificados que foram usados para nomes de domínio.</li> <li>● <b>false</b>: Obtenha os certificados que não foram usados para nenhum nome de domínio.</li> </ul> Padrão: <b>false</b>

Parâmetro	Obrigatório	Tipo	Descrição
exp_status	Não	Integer	Status do certificado. As opções são as seguintes: 0: não expirado; 1: expirado; 2: prestes a expirar (O certificado expirará dentro de um mês.)

## Parâmetros de solicitação

Tabela 4-427 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

Código de estado: 200

Tabela 4-428 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
items	Array of <b>CertificateBody</b> objects	Certificados
total	Integer	Número total de certificados

Tabela 4-429 CertificateBody

Parâmetro	Tipo	Descrição
id	String	ID do certificado.
name	String	Nome do certificado
expire_time	Long	Timestamp de expiração do certificado.

Parâmetro	Tipo	Descrição
exp_status	Integer	Status do certificado. O valor pode ser: <b>0</b> : O certificado é válido. <b>1</b> : O certificado expirou. <b>2</b> : O certificado expirará em um mês.
timestamp	Long	Carimbo de data e hora do upload do certificado.
bind_host	Array of <b>BindHost</b> objects	Nome de domínio associado ao certificado

**Tabela 4-430** BindHost

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio
waf_type	String	Modo de implantação da instância do WAF usado para o nome de domínio. O valor pode ser <b>cloud</b> para WAF na nuvem ou <b>premium</b> para instâncias dedicadas do WAF.
mode	String	Este parâmetro é requerido apenas pelo modo dedicado.

**Código de estado: 400**

**Tabela 4-431** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-432** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-433** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

OK

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

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.5.2 Carregamento de um certificado

### Função

Esta API é usada para carregar um certificado.

## URI

POST /v1/{project\_id}/waf/certificate

**Tabela 4-434** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

**Tabela 4-435** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-436** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json; charset=utf8</b>

**Tabela 4-437** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
name	Sim	String	Nome do certificado. O valor pode conter no máximo 64 caracteres. Somente dígitos, letras, hífens, (_), de sublinhados e pontos (.) são permitidos.
content	Sim	String	Arquivo do certificado. Somente certificados e arquivos de chave privada no formato PEM são suportados, e os caracteres de nova linha no arquivo devem ser substituídos por \n.
key	Sim	String	Chave privada do certificado. Somente certificados e arquivos de chave privada no formato PEM são suportados, e os caracteres de nova linha nos arquivos devem ser substituídos por \n.

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-438** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID do certificado
name	String	Nome do certificado
content	String	Arquivo de certificado, codificação PEM
key	String	Chave privada do certificado, que está no formato PEM.
expire_time	Long	Timestamp de expiração do certificado
exp_status	Integer	Status do certificado. As opções podem ser: <b>0</b> : O certificado não expirou. <b>1</b> : O certificado expirou. <b>2</b> : O certificado está prestes a expirar.
timestamp	Long	Timestamp de upload do certificado
bind_host	Array of <b>BindHost</b> objects	Nome de domínio associado ao certificado

**Tabela 4-439** BindHost

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio
waf_type	String	Modo de implantação da instância do WAF usado para o nome de domínio. O valor pode ser <b>cloud</b> para WAF na nuvem ou <b>premium</b> para instâncias dedicadas do WAF.
mode	String	Este parâmetro é requerido apenas pelo modo dedicado.

**Código de estado: 400**

**Tabela 4-440** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-441** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-442** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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



```
{
  "name" : "demo",
  "content" : "-----BEGIN CERTIFICATE----- \
\nMIIDyzCCArOgAwIBAgIJAN5U0Z4Bh5ccMA0GCSqGSIb3DQEBCwUAMHwxCzAJBgNV
BAYTA1pIMRiWEAYDVQQIDAIHVUFOR0RPTkcxETAPBgNVBAcMCMERPTkdHVUFOMQ0w
CwYDVQQKDARERUTFMQswCQYDVQQLEDAJESzELMAKGA1UEAwcT0QxHTAbBgkqhkiG
9w0BCQEWDk8IZC5odWF3ZWkuY29tMB4XDTIxMTEeXNTA4MTk0MVoXDTIyMTEeXNTA4
MTk0MVoWfDELMaKGA1UEBHMCMWkgxEjAQBGNVBAgMCUdVQU5HRE9ORzERMA8GA1UE
BwwIRE9OR0dVQU4xDTALBgNVBAoMBERFS0UxCzAJBgNVBAsMAkRMLQswCQYDVQQD
DAJPRDEdMBSGCSqGSIb3DQEJARYOTWhkLmhlYXdlas5jb20wggEiMA0GCSqGSIb3
DQEBAAQUAA4IBDwAwggEKAoIBAQCdcoLfk62//r0RHfYweYBj97S4NsJ8Qj0RG+Y02
OgwhQmRiNNjubJwP8Nqqyd86zr+fsSQxKBaBCosn1PcN2Pj2vPJD6NEk4I6VdOwr /
kFYm1OcmhSfW4wt6VakniOKIYGrCxxvQe1X2OyBxT+ocTLRgEIB8ZbvJyPNseg
feLEUuPYRrPQ5kXlGjH2/3NwZF0gBHVv/b0714fR+sWJmIA2yIjSBQ0DEAOSusXo FQ/
WRbBRH7DrQmxGiXsq4VELEr9Nnc/Kywq+9pYi8L+mKeRL+lcmMbxXC/3k60fMB
tVTiwcmS1Mkr3iG03i8u6H7RSvRwyBz9G9se+tmJZTPH61YtAgMBAAGjUDBOMB0G
A1UdDgQWBBQprUUFxW+gIkpzXdrYlswjfsSahWjAfBgNVHSMEGDAWgBQprUUFxW+g
IkpzXdrYlswjfsSahWjAMBGNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQA2
603KozsQoIKeLvgDjlcAXwWRFNw8SvlaSJAulhHgneMt9bQgIL+3PJWA/iMniOhU o/
kVwkiUicxw4t7RwP0hVms00Zw59MuqKd3oCSWkY04vEHs3t40JDWnGDnmQ4sol
RkOWJwL4w8tnPe3qY9JSupjlsu6Y1hlvKtEfn2vEKFNsuMhidkUpUAJWodHhWBQH
wgIDo4/6yTnWZNGK8Jda186Dm5IchXea1EoYBjShxiJb7HeWQ1kre+MCYi1RH0in 4mIXTr0oT4/
jWlGk1Sz6/ZhGRq+7W7tI17cvzCe+4XsvZienAcYoNd/WLfo91PD4 yAsRrXoJw1solBj0BkdZ\ \n
-----END CERTIFICATE-----",
  "key" : "-----BEGIN PRIVATE KEY----- \
\nMIIEEwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQCdcoLfk62//r0RH
FyweYBj97S4NsJ8Qj0RG+Y02OgwhQmRiNNjubJwP8Nqqyd86zr+fsSQxKBaBCosn
1PcN2Pj2vPJD6NEk4I6VdOwr/kFYm1OcmhSfW4wt6VakniOKIYGrCxxvQe1X2Oy BxT
+ocTLRgEIB8ZbvJyPNsegfeLEUuPYRrPQ5kXlGjH2/3NwZF0gBHVv/b0714fR+
sWJmIA2yIjSBQ0DEAOSusXoFQ/WRbBRH7DrQmxGiXsq4VELEr9Nnc/Kywq+9pYi 8L+mKeRL+lcmMbxXC/
3k60fMBtVTiwcmS1Mkr3iG03i8u6H7RSvRwyBz9G9se+tmJ ZTPH61YtAgMBAECggEBAL+xZxm/QoqXT
+2stoqV2GEYamFASpRqxlocjZMmEE/9 jZa
+cBWIjHhVpsjRqYfBDcHEebu0JwlrjcjIAvgnIvn05XgXm1A9Q+WbscokmcX1 xCvpHgc+MDVn
+uWdCd4KW5kEk4EnSsFN5iNSf+1VxNURN+gwSSp/0E+muwA5IISO G6HQ+p6qs52JAitX5t/
7ruKoHYXJxBnf7TUs7768qrh++KPKpPlq044qoYlCGOln 4urPBHunly04GgGw
+vkaqjqOvZrNLVOMMaFWBxsDWBehgSSBQTj+f3NCxneGYtt8 3SCTZQI5nIkb+r/
M455EwKTSXuEsNHoIwx7L6GEPbQECgYEA8IxgK2fYyKloICoh
TFJaRavvyjKa2+Aza4qT9SGY9Y30VPClPjBB1vUu5M9KrFufzlv06nGecHmpEwOe
8vbRu7nLAQTGYfi8VK63q8w6F1FdAyCG6Sx+BWCfWxJzXsZLAJTFklwi8HsOSlqh
6QNv0xbE2fLjXKf8MHvtrufip40CgYEA6sy87eDrkVgtq4ythAik3i1C5Z3v0fvx
mTb1G52Z21OyocNq3Tf/blZwoIclik6cyBzY6z1bIrbSzArCqm0sb2iD+kJL8100 /
qqdXjBxZuKkiVAMNNp7xJGZHHFKWuXT2+UX/tlyx4tT4dzrFTkdDXkcMmqfsRxd
lNEVaAaT8SECgYAoU7BptpIun43YtpfUfr3pSIN6oZeKoxSbw9i4MNC+4fSDRPC+ 80ImcmZRL7taF
+y7p0jxAOTuIkdJc8NbAiv5J9WzrwQ+5MF2BpB/2bYnRa6tNofH kZDy/
9bXys16qw2p5Ety8wVcgZTMvFMGiG/32IpZ65FYWEU8L5qSRwfFhQKBgQC9 ihjZTj/
bTHtRiHzppzCvyYm/Igd+Uwtsy0uXR1n0G1SQENgrTBD/J6AzdFJae6te P0U8YIM5Oqxf2i/as9ay
+IPRecM14eSxz7jJWAGx6Yx/3AZ+hAB1ZbNbqniCLYNk d0MvjwmA25ATO+ro40Z7AdEpQbk319aG/
WFyYBz9AQKBgQCucFPA115eslL8196V WMr2Qo0tqz17CGSoWQk2Sa2HZtZdfofXAaaqo
+zvJ6RPHtJh0jgJtx536DVV3egI 37YrdQyJbCPZXQ3SPgqWCorUnXBwq/
nxS06uwu6JBxUFc57ijmMU4fWYNrvkkmWb 7keAg/r5Uy1joMAvBN1I6lB8pg==\ \n
-----END
PRIVATE KEY-----"
}
```

## Exemplo de respostas

**Código de estado: 200**

OK

```
{
  "id" : "64af92e2087d49cbabc233e9bdc761b7",
  "name" : "testly",
  "timestamp" : 1658994431596,
  "expire_time" : 1682394560000
}
```

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.5.3 Consulta de um certificado

#### Função

Esta API é usada para consultar um certificado.

#### URI

GET /v1/{project\_id}/waf/certificate/{certificate\_id}

**Tabela 4-443** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
certificate_id	Sim	String	ID do certificado HTTPS. Ele pode ser obtido chamando a API <b>ListCertificates</b> .

Tabela 4-444 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <code>ListEnterpriseProject</code> do EPS.

## Parâmetros de solicitação

Tabela 4-445 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <code>X-Subject-Token</code> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json; charset=utf8</b>

## Parâmetros de resposta

Código de estado: 200

Tabela 4-446 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID do certificado
name	String	Nome do certificado
content	String	Arquivo de certificado, codificação PEM
key	String	Chave privada do certificado, que está no formato PEM.
expire_time	Long	Timestamp de expiração do certificado.
exp_status	Integer	Status do certificado. As opções podem ser: <b>0</b> : O certificado não expirou. <b>1</b> : O certificado expirou. <b>2</b> : O certificado está prestes a expirar.
timestamp	Long	Timestamp de upload do certificado
bind_host	Array of <b>BindHost</b> objects	Nome de domínio associado ao certificado

**Tabela 4-447 BindHost**

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio
waf_type	String	Modo de implantação da instância do WAF usado para o nome de domínio. O valor pode ser <b>cloud</b> para WAF na nuvem ou <b>premium</b> para instâncias dedicadas do WAF.
mode	String	Este parâmetro é requerido apenas pelo modo dedicado.

**Código de estado: 400**

**Tabela 4-448 Parâmetros do corpo de resposta**

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-449 Parâmetros do corpo de resposta**

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-450 Parâmetros do corpo de resposta**

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro



## 4.5.4 Modificação de um certificado

### Função

Esta API é usada para modificar um certificado.

### URI

PUT /v1/{project\_id}/waf/certificate/{certificate\_id}

**Tabela 4-451** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
certificate_id	Sim	String	ID do certificado HTTPS. Ele pode ser obtido chamando a API <b>ListCertificates</b> .

**Tabela 4-452** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

### Parâmetros de solicitação

**Tabela 4-453** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-454** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
name	Sim	String	Nome do certificado. O valor pode conter no máximo 64 caracteres. Somente dígitos, letras, hífen, (_), de sublinhados e pontos (.) são permitidos.
content	Não	String	Arquivo do certificado. Somente certificados e arquivos de chave privada no formato PEM são suportados, e os caracteres de nova linha no arquivo devem ser substituídos por \n.
key	Não	String	Chave privada do certificado. Somente certificados e arquivos de chave privada no formato PEM são suportados, e os caracteres de nova linha nos arquivos devem ser substituídos por \n.

## Parâmetros de resposta

### Código de estado: 200

**Tabela 4-455** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID do certificado
name	String	Nome do certificado
expire_time	Long	Timestamp quando o certificado expira
timestamp	Long	Timestamp.

### Código de estado: 400

**Tabela 4-456** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 401

Tabela 4-457 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 500

Tabela 4-458 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

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

## Exemplo de respostas

### Código de estado: 200

OK

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

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.



Código de status	Descrição
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.5.5 Exclusão de um certificado

### Função

Esta API é usada para excluir um certificado.

### URI

DELETE /v1/{project\_id}/waf/certificate/{certificate\_id}

**Tabela 4-459** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
certificate_id	Sim	String	ID do certificado HTTPS. Ele pode ser obtido chamando a API <b>ListCertificates</b> .

**Tabela 4-460** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-461** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-462** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID do certificado
name	String	Nome do certificado
content	String	Arquivo de certificado, codificação PEM
key	String	Chave privada do certificado no formato PEM
expire_time	Long	Timestamp de expiração do certificado
exp_status	Integer	Status do certificado. As opções podem ser: <b>0</b> : O certificado não expirou. <b>1</b> : O certificado expirou. <b>2</b> : O certificado está prestes a expirar.
timestamp	Long	Timestamp de upload do certificado
bind_host	Array of <b>BindHost</b> objects	Nome de domínio associado ao certificado

**Tabela 4-463** BindHost

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio

Parâmetro	Tipo	Descrição
waf_type	String	Modo de implantação da instância do WAF usado para o nome de domínio. O valor pode ser <b>cloud</b> para WAF na nuvem ou <b>premium</b> para instâncias dedicadas do WAF.
mode	String	Este parâmetro é requerido apenas pelo modo dedicado.

**Código de estado: 400**

**Tabela 4-464** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-465** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-466** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

OK

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

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.5.6 Aplicação de um certificado a um nome de domínio

### Função

Essa API é usada para aplicar um certificado a um nome de domínio.

### URI

POST /v1/{project\_id}/waf/certificate/{certificate\_id}/apply-to-hosts

**Tabela 4-467** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
certificate_id	Sim	String	ID do certificado HTTPS. Ele pode ser obtido chamando a API <b>ListCertificates</b> .

**Tabela 4-468** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

## Parâmetros de solicitação

**Tabela 4-469** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

**Tabela 4-470** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
cloud_host_ids	Não	Array of strings	ID do nome de domínio HTTPS no modo cloud. Você pode obtê-lo chamando a API <b>ListHost</b> .
premium_host_ids	Não	Array of strings	ID do nome de domínio HTTPS em modo dedicado. Você pode obtê-lo chamando a API <b>ListPremiumHost</b> .

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-471** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	ID do certificado.
name	String	Nome do certificado
timestamp	Long	Timestamp.

Parâmetro	Tipo	Descrição
expire_time	Long	Data de vencimento
bind_host	Array of <b>CertificateBundlingHostBody</b> objects	Lista de nomes de domínio

**Tabela 4-472** CertificateBundlingHostBody

Parâmetro	Tipo	Descrição
id	String	ID do nome de domínio
hostname	String	Nome de domínio
waf_type	String	Modo WAF (Cloud: cloud; Dedicado: premium) Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>cloud</b></li> <li>● <b>premium</b></li> </ul>

**Código de estado: 400**

**Tabela 4-473** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-474** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-475** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

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

## Exemplo de respostas

**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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.6 Gerenciamento de eventos

### 4.6.1 Consulta de lista de eventos de ataque

#### Função

Essa API é usada para consultar a lista de eventos de ataque. Atualmente, essa API não oferece suporte à consulta de todos os eventos de proteção. O parâmetro **pagesize** não pode ser definido como **-1**. Quanto maior o volume de dados, maior o consumo de memória. Um máximo de registros de dados de 10 000 pode ser consultado. Por exemplo, se o número de registros de dados em um período definido pelo usuário exceder 10 000 os dados cuja página é 101 (ou **pagesize** é maior que 100) não podem ser consultados. Você precisa ajustar o intervalo de tempo para um período mais longo e, em seguida, consultar os dados.

#### URI

GET /v1/{project\_id}/waf/event

Tabela 4-476 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

Tabela 4-477 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.



Parâmetro	Obrigatório	Tipo	Descrição
recent	Não	String	Intervalo de tempo para consulta de logs. Este parâmetro não pode ser usado em conjunto com <b>from</b> ou <b>to</b> ao mesmo tempo. Parâmetro <b>recent</b> deve ser usado com <b>from</b> ou <b>to</b> . Valores de enumeração: <ul style="list-style-type: none"> <li>● <b>yesterday</b></li> <li>● <b>today</b></li> <li>● <b>3days</b></li> <li>● <b>1week</b></li> <li>● <b>1month</b></li> </ul>
from	Não	Long	Hora de início (carimbo de data e hora de 13 dígitos). Este parâmetro deve ser usado junto com <b>to</b> , mas não pode ser usado junto com <b>recente</b> .
to	Não	Long	Hora de término (carimbo de data e hora de 13 dígitos). Este parâmetro deve ser usado em conjunto com <b>from</b> , mas não pode ser usado em conjunto com <b>recente</b> .

Parâmetro	Obrigatório	Tipo	Descrição
attacks	Não	Array	<p>Tipo de ataque</p> <ul style="list-style-type: none"> <li>● <b>vuln</b>: outros tipos de ataque</li> <li>● <b>sqli</b>: Ataques de injeção SQL</li> <li>● <b>lfi</b>: inclusão de arquivo local</li> <li>● <b>cmdi</b>: ataques de injeção de comando</li> <li>● <b>xss</b>: Ataques XSS</li> <li>● <b>robot</b>: rastreador malicioso</li> <li>● <b>rfi</b>: inclusão de arquivo remoto</li> <li>● <b>custom_custom</b>: ataque atingiu a regra de proteção de precisão</li> <li>● <b>cc</b>: Ataques CC</li> <li>● <b>webshell</b>: cavalo de Tróia do site</li> <li>● <b>custom_whiteblackip</b>: ataques que atingem a regra da lista de bloqueios e da lista de confiança</li> <li>● <b>custom_geoip</b>: ataques que atingem a regra de controle de acesso de geolocalização</li> <li>● <b>antitamper</b>: ataques que atingem a regra de prevenção de adulteração na web</li> <li>● <b>anticrawler</b>: ataques que atingem as regras anticrawler</li> <li>● <b>leakage</b>: ataques que atingem a regra de prevenção de vazamento de informações</li> <li>● <b>illegal</b>: pedidos ilegais</li> </ul>
hosts	Não	Array	<p>ID do nome de domínio. Ele pode ser obtido chamando a API <code>**ListHost</code>.</p>
page	Não	Integer	<p>Número de página dos dados a serem retornados durante a consulta de paginação. O valor padrão é <b>1</b>, indicando que os dados na primeira página são retornados.</p>

Parâmetro	Obrigatório	Tipo	Descrição
pagesize	Não	Integer	Número de resultados em cada página durante a consulta de paginação. Faixa de valor: <b>1 a 100</b> . O valor padrão é <b>10</b> , indicando que cada página contém 10 resultados.

## Parâmetros de solicitação

**Tabela 4-478** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json; charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-479** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	Número de eventos de ataque
items	Array of <b>ListEventItems</b> objects	Detalhes sobre um evento de ataque

**Tabela 4-480** ListEventItems

Parâmetro	Tipo	Descrição
id	String	ID do evento
time	Long	Contagem
policyid	String	ID da política

Parâmetro	Tipo	Descrição
sip	String	Endereço IP de origem, que é o endereço IP do visitante da web (endereço IP do invasor).
host	String	Nome de domínio atacado
url	String	URL atacada
attack	String	Tipo de ataque <ul style="list-style-type: none"> <li>● <b>vuln</b>: outros tipos de ataque</li> <li>● <b>sqli</b>: Ataque de injeção SQL</li> <li>● <b>lfi</b>: inclusão de arquivo local</li> <li>● <b>cmdi</b>: ataques de injeção de comando</li> <li>● <b>XSS</b>: Ataques XSS</li> <li>● <b>robot</b>: rastreador malicioso</li> <li>● <b>rfi</b>: inclusão de arquivo remoto</li> <li>● <b>custom_custom</b>: ataques atingem uma regra de proteção precisa</li> <li>● <b>webshell</b>: Trojan</li> <li>● <b>custom_blacklist</b>: ataques atingem uma regra de lista negra ou lista branca</li> <li>● <b>custom_geoip</b>: ataques atingem uma regra de controle de acesso de geolocalização</li> <li>● <b>antitamper</b>: ataques atingem uma regra de prevenção de adulteração na web</li> <li>● <b>anticrawler</b>: ataques atingem uma regra anticrawler</li> <li>● <b>leakage</b>: ataques atingem uma regra de prevenção de vazamento de informações</li> <li>● <b>illegal</b>: solicitações inválidas</li> </ul>
rule	String	ID da regra correspondente
payload	String	Acertar carga útil
payload_location	String	Bater posição de carga
action	String	Ação Protetora
request_line	String	Método de solicitação e caminho
headers	Object	Cabeçalho de solicitação HTTP
cookie	String	Solicitar cookie
status	String	Status do código de resposta
process_time	Integer	Tempo de processamento
region	String	Localização geográfica

Parâmetro	Tipo	Descrição
host_id	String	ID do nome de domínio
response_time	Long	Tempo para resposta
response_size	Integer	Tamanho do corpo da resposta
response_body	String	Corpo da resposta
request_body	String	Corpo da solicitação

#### Código de estado: 400

**Tabela 4-481** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

#### Código de estado: 401

**Tabela 4-482** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

#### Código de estado: 500

**Tabela 4-483** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

### 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-ec0c1fcdc52",
      "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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.6.2 Essa API é usada para consultar detalhes sobre um evento de um ID especificado.

### Função

Consulta de detalhes sobre um evento de uma ID especificada

### URI

GET /v1/{project\_id}/waf/event/{eventid}

**Tabela 4-484** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
eventid	Sim	String	ID do evento. Ele pode ser obtido chamando a API <b>ListEvent</b> .

**Tabela 4-485** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

### Parâmetros de solicitação

**Tabela 4-486** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).

Parâmetro	Obrigatório	Tipo	Descrição
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/ json; charset=utf8</b>

## Parâmetros de resposta

Código de estado: 200

Tabela 4-487 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	Número de eventos de ataque
items	Array of <a href="#">ShowEventItems</a> objects	Detalhes sobre um evento de ataque

Tabela 4-488 ShowEventItems

Parâmetro	Tipo	Descrição
time	Long	Timestamp quando o ataque ocorre, em milissegundos.
policyid	String	ID da política
sip	String	Endereço IP de origem
host	String	Nome de domínio
url	String	URL atacada
attack	String	Tipo de ataque
rule	String	ID da regra hit
action	String	Ação Protetora
cookie	String	Cookie do pedido de ataque
headers	Object	Cabeçalho da solicitação de ataque
host_id	String	ID do nome de domínio atacado
id	String	ID do evento
payload	String	Carga maliciosa
payload_location	String	Localização de carregamento malicioso



Parâmetro	Tipo	Descrição
region	String	Localização geográfica do endereço IP de origem
process_time	Integer	Tempo de processamento
request_line	String	Corpo do pedido de ataque
response_size	Integer	Tamanho do corpo da resposta (byte)
response_time	Long	Tempo de resposta (ms)
status	String	Código de resposta
request_body	String	Corpo da solicitação

#### Código de estado: 400

**Tabela 4-489** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

#### Código de estado: 401

**Tabela 4-490** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

#### Código de estado: 500

**Tabela 4-491** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

GET https://{Endpoint}/v1/{project\_id}/waf/event{event\_id}?enterprise\_project\_id=0

## Exemplo de respostas

**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-xxxxxxxx",
    "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,
    "process_time" : 0,
    "request_body" : "{}"
  } ]
}
```

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.7 Painel de controle

## 4.7.1 Consulta de estatísticas de solicitações e ataques

### Função

Consultando estatísticas de solicitações e ataques Observe que as API relacionadas ao painel não podem ser usadas para consultar dados por tempo personalizado. Somente os dados exibidos no console para ontem, hoje, últimos 3 dias, últimos 7 dias e últimos 30 dias podem ser consultados.

### URI

GET /v1/{project\_id}/waf/overviews/statistics

Tabela 4-492 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

Tabela 4-493 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.
from	Sim	Long	Hora de início (carimbo de data e hora de 13 dígitos). Este parâmetro deve ser usado junto com <b>to</b> .
to	Sim	Long	Hora de término (carimbo de data e hora de 13 dígitos). Este parâmetro deve ser usado junto com <b>from</b> .

Parâmetro	Obrigatório	Tipo	Descrição
hosts	Não	String	Os ID de nome de domínio. No modo de nuvem, os ID de nome de domínio podem ser obtidos chamando a API <b>ListHost</b> . No modo dedicado, os ID de nome de domínio podem ser obtidos chamando a API <b>ListPremiumHost</b> . Por padrão, esse parâmetro não é especificado e o número de solicitações e ataques de todos os nomes de domínio protegidos no projeto é consultado.
instances	Não	String	Os ID de instância que você deseja consultar. Esse parâmetro é necessário somente para instâncias dedicadas do WAF e instâncias de balanceamento de carga (modo ELB).

## Parâmetros de solicitação

Tabela 4-494 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

Código de estado: 200

Tabela 4-495 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
[items]	Array of <b>CountItem</b> objects	Estatísticas sobre solicitações e ataques no console do WAF

**Tabela 4-496** CountItem

Parâmetro	Tipo	Descrição
key	String	Tipo. As opções são <b>ACCESS</b> para solicitações totais, <b>CRAWLER</b> para mitigação de bot, <b>TOTAL_ATTACK</b> para ataques totais, <b>WEB_ATTACK</b> para proteção básica da web, <b>PRECISE</b> para proteção precisa, e <b>CC</b> para proteção contra ataques CC.
num	Integer	Quantidade.

**Código de estado: 400**

**Tabela 4-497** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-498** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 403**

**Tabela 4-499** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-500** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

Solicitação bem-sucedida.

```
[ {
  "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 status

Código de status	Descrição
200	Solicitação bem-sucedida.
400	Falha na solicitação.
401	O token não tem permissões necessárias.
403	A cota de recursos é insuficiente.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.7.2 Consulta de estatísticas do QPS

### Função

Esta API é usada para consultar o site QPS. Observe que as API relacionadas ao painel não podem ser usadas para consultar dados por tempo personalizado. Somente os dados exibidos no console para ontem, hoje, últimos 3 dias, últimos 7 dias e últimos 30 dias podem ser consultados.

### URI

GET /v1/{project\_id}/waf/overviews/qps/timeline

Tabela 4-501 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

Tabela 4-502 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Ele pode ser obtido chamando a API <b>ListEnterpriseProject</b> do EPS.
from	Sim	Long	Hora de início (13 dígitos timestamp em milissegundos). Este parâmetro deve ser usado junto com <b>to</b> .
to	Sim	Long	Hora de término (timestamp de 13 dígitos em milissegundos). Este parâmetro deve ser usado junto com <b>from</b> .

Parâmetro	Obrigatório	Tipo	Descrição
hosts	Não	String	Os ID de nome de domínio. No modo de nuvem, os ID de nome de domínio podem ser obtidos chamando a API <b>ListHost</b> . No modo dedicado, os ID de nome de domínio podem ser obtidos chamando a API <b>ListPremiumHost</b> . Por predefinição, este parâmetro não é especificado e os dados QPS de cada nome de domínio protegido no projecto são consultados.
instances	Não	String	Os ID de instância que você deseja consultar. Esse parâmetro é necessário somente para instâncias dedicadas do WAF e instâncias de balanceamento de carga (modo ELB).
group_by	Não	String	Dimensão de exibição. Por exemplo, o valor é <b>DAY</b> se os dados forem exibidos por dia.

## Parâmetros de solicitação

Tabela 4-503 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

Código de estado: 200



**Tabela 4-504** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
[items]	Array of <b>StatisticsTimelineItem</b> objects	Estatísticas do QPS ao longo do tempo no painel

**Tabela 4-505** StatisticsTimelineItem

Parâmetro	Tipo	Descrição
key	String	Valor da chave. As opções são <b>ACCESS</b> para solicitações totais, <b>CRAWLER</b> para mitigação de bot, <b>TOTAL_ATTACK</b> para ataques totais, <b>WEB_ATTACK</b> para proteção básica da Web, <b>PRECISE</b> para proteção precisa, <b>CC</b> para proteção contra ataques CC
timeline	Array of <b>TimeLineItem</b> objects	Dados estatísticos ao longo do tempo para o valor da chave correspondente

**Tabela 4-506** TimeLineItem

Parâmetro	Tipo	Descrição
time	Long	Data e hora
num	Integer	Quantidade.

**Código de estado: 400**

**Tabela 4-507** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-508** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-509** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.7.3 Consulta de estatísticas de uso da largura de banda

#### Função

Essa API é usada para consultar estatísticas de uso de largura de banda. Observe que as API relacionadas ao painel não podem ser usadas para consultar dados por tempo personalizado. Somente os dados exibidos no console para ontem, hoje, últimos 3 dias, últimos 7 dias e últimos 30 dias podem ser consultados.

#### URI

GET /v1/{project\_id}/waf/overviews/bandwidth/timeline

**Tabela 4-510** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

**Tabela 4-511** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.
from	Sim	Long	Hora de início (13 dígitos timestamp em milissegundos). Este parâmetro deve ser usado junto com <b>to</b> .
to	Sim	Long	Hora de término (timestamp de 13 dígitos em milissegundos). Este parâmetro deve ser usado junto com <b>from</b> .
hosts	Não	String	Os ID de nome de domínio. No modo de nuvem, os ID de nome de domínio podem ser obtidos chamando a API <b>ListHost</b> . No modo dedicado, os ID de nome de domínio podem ser obtidos chamando a API <b>ListPremiumHost</b> . Por padrão, esse parâmetro não é especificado e os dados de uso de largura de banda de cada nome de domínio protegido no projeto são consultados.
instances	Não	String	Os ID de instância que você deseja consultar. Esse parâmetro é necessário somente para instâncias dedicadas do WAF e instâncias de balanceamento de carga (modo ELB).
group_by	Não	String	Dimensão de exibição. Por exemplo, se o valor for <b>DAY</b> , os dados serão exibidos por dia.

## Parâmetros de solicitação

**Tabela 4-512** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).

Parâmetro	Obrigatório	Tipo	Descrição
Content-Type	Sim	String	Tipo de conteúdo Padrão: <b>application/ json; charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-513** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
[items]	Array of <b>BandwidthStatisticsTimelineItem</b> objects	Estatísticas de largura de banda ao longo do tempo

**Tabela 4-514** BandwidthStatisticsTimelineItem

Parâmetro	Tipo	Descrição
key	String	Valor da chave. As opções são <b>BANDWIDTH</b> , <b>IN_BANDWIDTH</b> , e <b>OUT_BANDWIDTH</b> .
timeline	Array of <b>TimeLineItem</b> objects	Estatísticas da linha do tempo do valor da chave correspondente.

**Tabela 4-515** TimeLineItem

Parâmetro	Tipo	Descrição
time	Long	Data e hora
num	Integer	Quantidade.

**Código de estado: 400**

**Tabela 4-516** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro

Parâmetro	Tipo	Descrição
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-517** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-518** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.7.4 Consulta de estatísticas das principais exceções

#### Função

Essa API é usada para consultar as principais exceções de serviços, como solicitações ou erros anormais. Observe que as API relacionadas ao painel não podem ser usadas para consultar dados por tempo personalizado. Somente os dados exibidos no console para ontem, hoje, últimos 3 dias, últimos 7 dias e últimos 30 dias podem ser consultados.

#### URI

GET /v1/{project\_id}/waf/overviews/abnormal

**Tabela 4-519** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

**Tabela 4-520** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.

Parâmetro	Obrigatório	Tipo	Descrição
from	Sim	Long	Hora de início (13 dígitos timestamp em milissegundos). Este parâmetro deve ser usado junto com <b>to</b> .
to	Sim	Long	Hora de término (timestamp de 13 dígitos em milissegundos). Este parâmetro deve ser usado junto com <b>from</b> .
top	Não	Integer	N principais resultados a serem consultados. O valor padrão é 5 e o valor máximo é 10.
code	Não	Integer	Código de erro a ser consultado. Atualmente, 404, 500 e 502 são suportados. Se esse parâmetro não for especificado, o código de status 404 é consultado por padrão.
hosts	Não	String	Os ID de nome de domínio. No modo de nuvem, os ID de nome de domínio podem ser obtidos chamando a API <b>ListHost</b> . No modo dedicado, os ID de nome de domínio podem ser obtidos chamando a API <b>ListPremiumHost</b> . Por padrão, esse parâmetro não é necessário e os dados estatísticos de todos os nomes de domínio protegidos no projeto são consultados.
instances	Não	String	IDs de instância que você deseja consultar. Esse parâmetro é necessário somente para instâncias dedicadas do WAF e instâncias de balanceamento de carga (modo ELB).



## Parâmetros de solicitação

**Tabela 4-521** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-522** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	Número de solicitações anormais
items	Array of <b>UrlCountItem</b> objects	Matriz de informações de solicitação anormais.

**Tabela 4-523** UrlCountItem

Parâmetro	Tipo	Descrição
key	String	Tipo de ataque.
num	Integer	Quantidade.
host	String	Nomes de domínio protegidos

**Código de estado: 400**

**Tabela 4-524** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 401

**Tabela 4-525** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 500

**Tabela 4-526** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

### 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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.

Código de status	Descrição
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.7.5 Consulta de principais estatísticas de segurança por categoria

### Função

Essa API é usada para consultar estatísticas por categoria, incluindo o nome de domínio atacado, o endereço IP da origem do ataque, o URL atacado, a região da origem do ataque e a distribuição do evento de ataque. Observe que as API relacionadas ao painel não podem ser usadas para consultar dados por tempo personalizado. Somente os dados exibidos no console para ontem, hoje, últimos 3 dias, últimos 7 dias e últimos 30 dias podem ser consultados.

### URI

GET /v1/{project\_id}/waf/overviews/classification

**Tabela 4-527** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

**Tabela 4-528** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.
from	Sim	Long	Hora de início (13 dígitos timestamp em milissegundos). Este parâmetro deve ser usado junto com <b>to</b> .

Parâmetro	Obrigatório	Tipo	Descrição
to	Sim	Long	Hora de término (timestamp de 13 dígitos em milissegundos). Este parâmetro deve ser usado junto com <b>from</b> .
top	Não	Integer	Os primeiros vários resultados que você deseja consultar. Valor máximo: <b>10</b> . Valor padrão: <b>5</b> .
hosts	Não	String	Os ID de nome de domínio. No modo de nuvem, os ID de nome de domínio podem ser obtidos chamando a API <b>ListHost</b> . No modo dedicado, os ID de nome de domínio podem ser obtidos chamando a API <b>ListPremiumHost</b> . Por padrão, esse parâmetro não é necessário e os dados estatísticos de todos os nomes de domínio protegidos no projeto são consultados. Para consultar dados sobre vários nomes de domínio especificados, consulte o exemplo de solicitação.
instances	Não	String	Os ID de instância que você deseja consultar. Esse parâmetro é necessário somente para instâncias dedicadas do WAF e instâncias de balanceamento de carga (modo ELB).

## Parâmetros de solicitação

Tabela 4-529 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-530** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
domain	<b>DomainClassificationItem</b> object	Nome de domínio atacado
attack_type	<b>AttackTypeClassificationItem</b> object	Distribuição de eventos de ataque
ip	<b>IpClassificationItem</b> object	Atacar o endereço IP de origem
url	<b>UrlClassificationItem</b> object	Atacar URL
geo	<b>GeoClassificationItem</b> object	Região de origem

**Tabela 4-531** DomainClassificationItem

Parâmetro	Tipo	Descrição
total	Integer	Número total de DomainItem
items	Array of <b>DomainItem</b> objects	Detalhes do DomainItem

**Tabela 4-532** DomainItem

Parâmetro	Tipo	Descrição
key	String	Nome de domínio
num	Integer	Quantidade.
web_tag	String	Nome do site, que é o mesmo que o nome do site nos detalhes do nome de domínio no console do WAF.

**Tabela 4-533** AttackTypeClassificationItem

Parâmetro	Tipo	Descrição
total	Integer	Número total de AttackTypeItem
items	Array of <a href="#">AttackTypeItem</a> objects	Detalhes do AttackTypeItem

**Tabela 4-534** AttackTypeItem

Parâmetro	Tipo	Descrição
key	String	Tipo de ataque
num	Integer	Quantidade.

**Tabela 4-535** IpClassificationItem

Parâmetro	Tipo	Descrição
total	Integer	Número total de IpItem
items	Array of <a href="#">IpItem</a> objects	Detalhes do IpItem

**Tabela 4-536** IpItem

Parâmetro	Tipo	Descrição
key	String	Endereço IP.
num	Integer	Quantidade.

**Tabela 4-537** UrlClassificationItem

Parâmetro	Tipo	Descrição
total	Integer	Número total de UrlItem
items	Array of <a href="#">UrlItem</a> objects	Detalhes do UrlItem

**Tabela 4-538** UriItem

Parâmetro	Tipo	Descrição
key	String	Caminho do URL.
num	Integer	Quantidade.
host	String	Nome de domínio

**Tabela 4-539** GeoClassificationItem

Parâmetro	Tipo	Descrição
total	Integer	Número total de GeoItem
items	Array of <b>GeoItem</b> objects	Detalhes do GeoItem

**Tabela 4-540** GeoItem

Parâmetro	Tipo	Descrição
key	String	Região de origem
num	Integer	Quantidade.

**Código de estado: 400**

**Tabela 4-541** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-542** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-543** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Exemplos de solicitações**

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/classification?
enterprise_project_id=0&from=1652889600354&to=1655435681354&top=10&hosts=1bac09440
a814aa98ed08302c580a48b&hosts=5a532f83a2fb476ba51ca1de7b1ebc43
```

**Exemplo de respostas**

**Código de estado: 200**

OK

```
{
  "attack_type" : {
    "total" : 1,
    "items" : [ {
      "key" : "custom_custom",
      "num" : 2
    } ]
  },
  "domain" : {
    "total" : 2,
    "items" : [ {
      "key" : "www.whitelist.com",
      "num" : 2,
      "web_tag" : "www.whitelist.com"
    }, {
      "key" : "zbx002.apayaduo.cn",
      "num" : 2,
      "web_tag" : ""
    } ]
  },
  "geo" : {
    "total" : 1,
    "items" : [ {
      "key" : "Shanghai",
      "num" : 2
    } ]
  },
  "ip" : {
    "total" : 1,
    "items" : [ {
      "key" : "10.142.4.15",
      "num" : 2
    } ]
  },
  "url" : {
    "total" : 1,
    "items" : [ {
      "key" : "/attack",
      "num" : 2,
      "host" : "www.whitelist.com"
    } ]
  }
}
```



```
}  
}
```

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.7.6 Consulta de solicitações de sites

### Função

Esta API é usada para consultar solicitações de sites. Observe que as API relacionadas ao painel não podem ser usadas para consultar dados por tempo personalizado. Somente os dados exibidos no console para ontem, hoje, últimos 3 dias, últimos 7 dias e últimos 30 dias podem ser consultados.

### URI

GET /v1/{project\_id}/waf/overviews/request/timeline

**Tabela 4-544** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

**Tabela 4-545** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.
from	Sim	Long	Hora de início (13 dígitos timestamp em milissegundos). Este parâmetro deve ser usado junto com <b>to</b> .
to	Sim	Long	Hora de término (timestamp de 13 dígitos em milissegundos). Este parâmetro deve ser usado junto com <b>from</b> .
hosts	Não	Array	Os ID de nome de domínio. No modo de nuvem, os ID de nome de domínio podem ser obtidos chamando a API <b>ListHost</b> . No modo dedicado, os ID de nome de domínio podem ser obtidos chamando a API <b>ListPremiumHost</b> . Por padrão, esse parâmetro não é necessário e os dados estatísticos de todos os nomes de domínio protegidos no projeto são consultados. Para consultar dados sobre vários nomes de domínio especificados, consulte o exemplo de solicitação.
instances	Não	Array	Os ID de instância que você deseja consultar. Esse parâmetro é necessário somente para instâncias dedicadas do WAF e instâncias de balanceamento de carga (modo ELB).
group_by	Não	String	Como os dados são exibidos. Para exibir dados por dia, defina o parâmetro como <b>DAY</b> . Por padrão, esse parâmetro não é especificado e os dados são exibidos por minuto.

## Parâmetros de solicitação

**Tabela 4-546** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-547** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
[items]	Array of <b>StatisticsTimelineItem</b> objects	Solicitar Dados de Cronograma para Estatísticas de Segurança.

**Tabela 4-548** StatisticsTimelineItem

Parâmetro	Tipo	Descrição
key	String	Valor da chave. As opções são <b>ACCESS</b> para solicitações totais, <b>CRAWLER</b> para mitigação de bot, <b>TOTAL_ATTACK</b> para ataques totais, <b>WEB_ATTACK</b> para proteção básica da Web, <b>PRECISE</b> para proteção precisa, <b>CC</b> para proteção contra ataques CC
timeline	Array of <b>TimeLineItem</b> objects	Dados estatísticos ao longo do tempo para o valor da chave correspondente

**Tabela 4-549** TimeLineItem

Parâmetro	Tipo	Descrição
time	Long	Data e hora

Parâmetro	Tipo	Descrição
num	Integer	Quantidade.

**Código de estado: 400**

**Tabela 4-550** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-551** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-552** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/request/timeline?
enterprise_project_id=0&from=1650470400196&to=1650470450000
```

## Exemplo de respostas

**Código de estado: 200**

OK

```
[ {
  "key" : "ACCESS",
  "timeline" : [ {
    "time" : 1650470400196,
```

```

    "num" : 0
  } ]
}, {
  "key" : "PRECISE",
  "timeline" : [ {
    "time" : 1650470400196,
    "num" : 0
  } ]
}, {
  "key" : "CRAWLER",
  "timeline" : [ {
    "time" : 1650470400196,
    "num" : 0
  } ]
}, {
  "key" : "CC",
  "timeline" : [ {
    "time" : 1650470400196,
    "num" : 0
  } ]
}, {
  "key" : "TOTAL_ATTACK",
  "timeline" : [ {
    "time" : 1650470400000,
    "num" : 0
  } ]
}, {
  "key" : "WEB_ATTACK",
  "timeline" : [ {
    "time" : 1650470400196,
    "num" : 0
  } ]
} ]

```

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.8 Consulta de nome de domínio de um inquilino

## 4.8.1 Consulta de nomes de domínio protegidos com todas as instâncias do WAF

### Função

Essa API é usada para consultar a lista de nomes de domínio de proteção.

### URI

GET /v1/{project\_id}/composite-waf/host

**Tabela 4-553** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

**Tabela 4-554** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API <b>ListEnterpriseProject</b> do EPS.
page	Não	Integer	Número de página dos dados a serem retornados durante a consulta de paginação. O valor padrão é <b>1</b> , indicando que os dados na primeira página são retornados. Padrão: <b>1</b>
pagesize	Não	Integer	Número de resultados em cada página durante a consulta de paginação. Faixa de valor: <b>1 a 100</b> . O valor padrão é <b>10</b> , indicando que cada página contém 10 resultados. Padrão: <b>10</b>
hostname	Não	String	Nome de domínio
policyname	Não	String	Nome da política

Parâmetro	Obrigatório	Tipo	Descrição
protect_status	Não	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>
waf_type	Não	String	Modo WAF do nome de domínio
is_https	Não	Boolean	Se HTTPS é usado para o nome de domínio

## Parâmetros de solicitação

Tabela 4-555 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-556** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total	Integer	Número de todos os nomes de domínio protegidos
cloud_total	Integer	Número de nomes de domínio protegidos com o WAF na nuvem
premium_total	Integer	Número de nomes de domínio protegidos com instâncias WAF dedicadas
items	Array of <b>CompositeHostResponse</b> objects	Detalhes sobre o nome de domínio protegido

**Tabela 4-557** CompositeHostResponse

Parâmetro	Tipo	Descrição
id	String	<ul style="list-style-type: none"> <li>● <b>false</b>: O endereço IP exclusivo não é prático.</li> </ul>
hostid	String	ID do nome de domínio
hostname	String	Nome de domínio adicionado ao WAF na nuvem.
policyid	String	ID da política
access_code	String	Prefixo CNAME
protect_status	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>
access_status	Integer	Status de acesso ao nome de domínio. O valor pode ser <b>0</b> ou <b>1</b> . <b>0</b> : O tráfego do site não foi encaminhado para o WAF. <b>1</b> : O tráfego do site foi encaminhado para o WAF.
proxy	Boolean	Se um proxy é usado para o nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>false</b>: Nenhum proxy é usado.</li> <li>● <b>true</b>: Um proxy é usado.</li> </ul>



Parâmetro	Tipo	Descrição
timestamp	Long	Hora em que o nome de domínio foi adicionado ao WAF.
paid_type	String	Modo de pagamento baseado em pacote. Atualmente, apenas o modo pré-pago é suportado.
flag	<b>Flag</b> object	Identificador especial, que é usado no console.
waf_type	String	Modo de WAF usado para proteger o nome de domínio. O valor pode ser <b>cloud</b> ou <b>premium</b> . <b>cloud</b> : O WAF na nuvem é usado para proteger o domínio. <b>premium</b> : Uma instância dedicada do WAF é usada para proteger o nome de domínio.
web_tag	String	Nome do site, que é o mesmo que o nome do site nos detalhes do nome de domínio no console do WAF.
access_progress	Array of <b>Access_progress</b> objects	Progresso do acesso, que é usado apenas para o novo console do WAF.
premium_waf_instances	Array of <b>Premium_waf_instances</b> objects	Lista de instâncias WAF dedicadas
description	String	Descrição do nome de domínio
exclusive_ip	Boolean	Se usar um endereço IP exclusivo. <ul style="list-style-type: none"> <li>● <b>true</b>: O endereço IP exclusivo é usado.</li> <li>● <b>false</b>: O endereço IP exclusivo não é prático.</li> </ul>
region	String	ID da região. Esse parâmetro é incluído quando o nome de domínio é adicionado ao WAF por meio do console. Esse parâmetro é deixado em branco quando o nome de domínio é adicionado ao WAF ao chamar uma API. Você pode consultar o ID da região na página Regiões e Endpoints no site da Huawei Cloud.

**Tabela 4-558** Bandeira

Parâmetro	Tipo	Descrição
pci_3ds	String	<p>Se o site passa a verificação de certificação PCI 3DS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI 3DS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação do PCI 3DS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
pci_dss	String	<p>Se o site passou na verificação de certificação PCI DSS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI DSS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação PCI DSS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cname	String	<p>O registro CNAME que está sendo usado.</p> <ul style="list-style-type: none"> <li>● <b>old</b>: O registro CNAME antigo é usado.</li> <li>● <b>new</b>: O novo registro CNAME é usado.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>old</b></li> <li>● <b>new</b></li> </ul>
is_dual_az	String	<p>Se o WAF suporta o Multi-AZ DR</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O WAF suporta DR multi-AZ.</li> <li>● <b>false</b>: O WAF não suporta DR multi-AZ.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ipv6	String	<p>Se a proteção IPv6 é suportada.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>

**Tabela 4-559** Access\_progress

Parâmetro	Tipo	Descrição
step	Integer	Etapa
status	Integer	Estado. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: O passo não foi concluído.</li> <li>● <b>1</b>: O passo terminou.</li> </ul>

**Tabela 4-560** Premium\_waf\_instances

Parâmetro	Tipo	Descrição
id	String	ID da instância dedicada do WAF
name	String	Nome da instância dedicada do WAF
accessed	Boolean	Se o nome de domínio é adicionado à instância dedicada do WAF. As opções são <b>true</b> e <b>false</b> . <ul style="list-style-type: none"> <li>● <b>true</b>: O nome de domínio foi adicionado ao WAF.</li> <li>● <b>false</b>: O nome de domínio não foi adicionado ao WAF.</li> </ul>

**Código de estado: 400**

**Tabela 4-561** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-562** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-563** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

OK

```
{
  "items" : [ {
    "id" : "31af669f567246c289771694f2112289",
    "hostid" : "31af669f567246c289771694f2112289",
    "description" : "",
    "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"
  } ],
  "total" : 1,
  "cloud_total" : 1,
  "premium_total" : 0
}
```

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

### 4.8.2 Consulta de um nome de domínio por ID

#### Função

Essa API é usada para consultar um nome de domínio protegido por ID.

#### URI

GET /v1/{project\_id}/composite-waf/host/{host\_id}

**Tabela 4-564** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.
host_id	Sim	String	ID do nome de domínio. No modo nuvem, ele pode ser obtido chamando a API ListHost. No modo dedicado, ele pode ser obtido chamando a API ListPremiumHost.

**Tabela 4-565** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	Você pode obter o ID chamando a API ListEnterpriseProject do EPS.

## Parâmetros de solicitação

**Tabela 4-566** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json;charset=utf8</b>

## Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-567** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
id	String	<ul style="list-style-type: none"> <li>● <b>false</b>: O endereço IP exclusivo não é prático.</li> </ul>
hostid	String	ID do nome de domínio
hostname	String	Nome de domínio adicionado ao WAF na nuvem.
policyid	String	ID da política
access_code	String	Prefixo CNAME
protect_status	Integer	Status do WAF do nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>-1</b>: A proteção WAF é ignorada. As solicitações do nome de domínio são enviadas diretamente para o servidor de backend e não passam pelo WAF.</li> <li>● <b>0</b>: A proteção WAF está suspensa. O WAF encaminha apenas solicitações destinadas ao nome de domínio e não detecta ataques.</li> <li>● <b>1</b>: A proteção WAF está ativada. O WAF detecta ataques com base na política configurada.</li> </ul>
access_status	Integer	Status de acesso ao nome de domínio. O valor pode ser <b>0</b> ou <b>1</b> . <b>0</b> : O tráfego do site não foi encaminhado para o WAF. <b>1</b> : O tráfego do site foi encaminhado para o WAF.

Parâmetro	Tipo	Descrição
proxy	Boolean	Se um proxy é usado para o nome de domínio protegido. <ul style="list-style-type: none"> <li>● <b>false</b>: Nenhum proxy é usado.</li> <li>● <b>true</b>: Um proxy é usado.</li> </ul>
timestamp	Long	Hora em que o nome de domínio foi adicionado ao WAF.
paid_type	String	Modo de pagamento baseado em pacote. Atualmente, apenas o modo pré-pago é suportado.
flag	<b>Flag</b> object	Identificador especial, que é usado no console.
waf_type	String	Modo de WAF usado para proteger o nome de domínio. O valor pode ser <b>cloud</b> ou <b>premium</b> . <b>cloud</b> : O WAF na nuvem é usado para proteger o domínio. <b>premium</b> : Uma instância dedicada do WAF é usada para proteger o nome de domínio.
web_tag	String	Nome do site, que é o mesmo que o nome do site nos detalhes do nome de domínio no console do WAF.
access_progress	Array of <b>Access_progress</b> objects	Progresso do acesso, que é usado apenas para o novo console do WAF.
premium_waf_instances	Array of <b>Premium_waf_instances</b> objects	Lista de instâncias WAF dedicadas
description	String	Descrição do nome de domínio
exclusive_ip	Boolean	Se usar um endereço IP exclusivo. <ul style="list-style-type: none"> <li>● <b>true</b>: O endereço IP exclusivo é usado.</li> <li>● <b>false</b>: O endereço IP exclusivo não é prático.</li> </ul>
region	String	ID da região. Esse parâmetro é incluído quando o nome de domínio é adicionado ao WAF por meio do console. Esse parâmetro é deixado em branco quando o nome de domínio é adicionado ao WAF ao chamar uma API. Você pode consultar o ID da região na página Regiões e Endpoints no site da Huawei Cloud.

**Tabela 4-568** Bandeira

Parâmetro	Tipo	Descrição
pci_3ds	String	<p>Se o site passa a verificação de certificação PCI 3DS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI 3DS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação do PCI 3DS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
pci_dss	String	<p>Se o site passou na verificação de certificação PCI DSS.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O site passou na verificação de certificação PCI DSS.</li> <li>● <b>false</b>: O site falhou na verificação de certificação PCI DSS.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
cname	String	<p>O registro CNAME que está sendo usado.</p> <ul style="list-style-type: none"> <li>● <b>old</b>: O registro CNAME antigo é usado.</li> <li>● <b>new</b>: O novo registro CNAME é usado.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>old</b></li> <li>● <b>new</b></li> </ul>
is_dual_az	String	<p>Se o WAF suporta o Multi-AZ DR</p> <ul style="list-style-type: none"> <li>● <b>true</b>: O WAF suporta DR multi-AZ.</li> <li>● <b>false</b>: O WAF não suporta DR multi-AZ.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>
ipv6	String	<p>Se a proteção IPv6 é suportada.</p> <ul style="list-style-type: none"> <li>● <b>true</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul> <p>Valores de enumeração:</p> <ul style="list-style-type: none"> <li>● <b>true</b></li> <li>● <b>false</b></li> </ul>



**Tabela 4-569** Access\_progress

Parâmetro	Tipo	Descrição
step	Integer	Etapa
status	Integer	Estado. O valor pode ser <b>0</b> ou <b>1</b> . <ul style="list-style-type: none"> <li>● <b>0</b>: O passo não foi concluído.</li> <li>● <b>1</b>: O passo terminou.</li> </ul>

**Tabela 4-570** Premium\_waf\_instances

Parâmetro	Tipo	Descrição
id	String	ID da instância dedicada do WAF
name	String	Nome da instância dedicada do WAF
accessed	Boolean	Se o nome de domínio é adicionado à instância dedicada do WAF. As opções são <b>true</b> e <b>false</b> . <ul style="list-style-type: none"> <li>● <b>true</b>: O nome de domínio foi adicionado ao WAF.</li> <li>● <b>false</b>: O nome de domínio não foi adicionado ao WAF.</li> </ul>

**Código de estado: 400**

**Tabela 4-571** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 401**

**Tabela 4-572** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

**Código de estado: 500**

**Tabela 4-573** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

**Código de estado: 200**

OK

```
{
  "id" : "31af669f567246c289771694f2112289",
  "hostid" : "31af669f567246c289771694f2112289",
  "description" : "",
  "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 status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).

## 4.9 Consulta de recursos disponíveis em um site

### 4.9.1 Recursos de consulta disponíveis em um site

#### Função

Esta API é usada para consultar os recursos disponíveis em um site específico.

#### URI

GET /v1/{project\_id}/waf/config/console

Tabela 4-574 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Para obtê-lo, vá para o console de gerenciamento do Huawei Cloud e passe o cursor sobre seu nome de usuário. Na janela exibida, escolha <b>My Credentials</b> . Em seguida, na área <b>Projects</b> , visualize <b>Project ID</b> correspondente.

#### Parâmetros de solicitação

Tabela 4-575 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM (valor de <b>X-Subject-Token</b> no cabeçalho da resposta).
Content-Type	Sim	String	Tipo de conteúdo. Padrão: <b>application/json; charset=utf8</b>

#### Parâmetros de resposta

**Código de estado: 200**

**Tabela 4-576** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
eps	Boolean	Se o EPS é suportado. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: EPS é suportado.</li> <li>● <b>false</b>: EPS não é suportado.</li> </ul>
tls	Boolean	Se deve suportar a versão TLS. O valor pode ser <b>true</b> ou <b>false</b> . Se você defini-lo como <b>true</b> , você pode configurar TLS v1.0, TLS v1.1 ou TLS v1.2. O valor padrão é <b>TLS v1.0</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: A versão TLS é suportada.</li> <li>● <b>false</b>: A versão TLS não é suportada.</li> </ul>
ipv6	Boolean	Se a proteção IPv6 é suportada. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: A proteção IPv6 é suportada.</li> <li>● <b>false</b>: A proteção IPv6 não é suportada.</li> </ul>
alert	Boolean	Se o relatório de alarme é suportado. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: Relatório de alarme é suportado.</li> <li>● <b>false</b>: Relatórios de alarme não são suportados.</li> </ul>
custom	Boolean	Se a proteção precisa é suportada. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: Proteção precisa é suportada.</li> <li>● <b>false</b>: A proteção precisa não é suportada.</li> </ul>
elb_mode	Boolean	Se o modo ELB é suportado. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: O modo ELB é suportado.</li> <li>● <b>false</b>: O modo ELB não é suportado.</li> </ul>
event_lts	Boolean	Se o registro LTS é suportado. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: O registro LTS é suportado.</li> <li>● <b>false</b>: O registro LTS não é suportado.</li> </ul>
multi_dns	Boolean	Se a resolução multi-DNS é suportada. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: A resolução multi-DNS é suportada.</li> <li>● <b>false</b>: A resolução multi-DNS não é suportada.</li> </ul>
search_ip	Boolean	Se a pesquisa de endereço IP é suportada. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: A pesquisa de endereço IP é suportada.</li> <li>● <b>false</b>: A pesquisa de endereço IP não é suportada.</li> </ul>

Parâmetro	Tipo	Descrição
cc_enhance	Boolean	Se a proteção contra ataque CC é suportada. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: A proteção contra ataques CC é suportada.</li> <li>● <b>false</b>: A proteção contra ataques CC não é suportada.</li> </ul>
cname_switch	Boolean	Se o switchover CNAME é suportado. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: O switchover CNAME é suportado.</li> <li>● <b>false</b>: O switchover CNAME não é suportado.</li> </ul>
custom_block	Boolean	Se a página de bloco personalizada é suportada. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: A página de blocos personalizados é suportada.</li> <li>● <b>false</b>: A página de bloco personalizada não é suportada.</li> </ul>
advanced_ignore	Boolean	Se o mascaramento de alarme falso é suportado. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: O mascaramento de alarme falso é suportado.</li> <li>● <b>false</b>: O mascaramento de alarme falso não é suportado.</li> </ul>
js_crawler_enable	Boolean	Se o anti-crawler baseado em JavaScript é suportado. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: O anti-crawler baseado em JavaScript é suportado.</li> <li>● <b>false</b>: O anti-crawler baseado em JavaScript não é suportado.</li> </ul>
deep_decode_enable	Boolean	Se a inspeção profunda na proteção básica da web é suportada. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: A inspeção profunda é suportada.</li> <li>● <b>false</b>: A inspeção profunda não é suportada.</li> </ul>
overview_bandwidth	Boolean	Se a resolução em profundidade é suportada. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: A resolução em profundidade é suportada.</li> <li>● <b>false</b>: A resolução em profundidade não é suportada.</li> </ul>

Parâmetro	Tipo	Descrição
proxy_use_oldcname	Boolean	Se a resolução CNAME antiga é suportada. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: A antiga resolução CNAME é suportada.</li> <li>● <b>false</b>: A resolução CNAME antiga não é suportada.</li> </ul>
check_all_headers_enable	Boolean	Se a inspeção de cabeçalho é suportada. As opções são <b>false</b> e <b>true</b> . <ul style="list-style-type: none"> <li>● <b>True</b>: A inspeção do cabeçalho é suportada.</li> <li>● <b>false</b>: A inspeção de cabeçalho não é suportada.</li> </ul>
geoip_enable	Boolean	Seja para suportar o controle de acesso de geolocalização. As opções são falsas: não suportadas; verdadeiras: suportadas.
load_balance_enable	Boolean	Se deve suportar o balanceamento de carga de acesso ao nome de domínio. As opções são falsas: não suportadas; verdadeiras: suportadas.
ipv6_protection_enable	Boolean	Se a defesa IPv6 é suportada. As opções são falsas: não suportadas; verdadeiras: suportadas.
policy_sharing_enable	Boolean	Seja para apoiar o compartilhamento de políticas. As opções são falsas: não suportadas; verdadeiras: suportadas.
ip_group	Boolean	Se o grupo de endereços IP é suportado. As opções são falsas: não suportadas; verdadeiras: suportadas.
robot_action_enable	Boolean	Se a apoiar site anti-crawler. As opções são falsas: não suportadas; verdadeiras: suportadas.
http2_enable	Boolean	Suportar ou não HTTP2. As opções são falsas: não suportadas; verdadeiras: suportadas.
timeout_config_enable	Boolean	Se deve ou não suportar a configuração de timeout. As opções são falsas: não suportadas; verdadeiras: suportadas.

**Código de estado: 400**

**Tabela 4-577** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 401

Tabela 4-578 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

### Código de estado: 500

Tabela 4-579 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	String	Código de erro
error_msg	String	Mensagem de erro

## Exemplos de solicitações

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

## Exemplo de respostas

### 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,
  "cc_enhance" : true,
  "cname_switch" : true,
  "custom_block" : true,
  "geoip_enable" : true,
  "http2_enable" : true,
  "advanced_ignore" : true,
  "js_crawler_enable" : true,
  "deep_decode_enable" : true,
  "overview_bandwidth" : true,
  "proxy_use_oldcname" : false,
  "load_balance_enable" : true,
  "robot_action_enable" : true,
  "policy_sharing_enable" : true,
  "timeout_config_enable" : true,
  "ipv6_protection_enable" : true,
  "check_all_headers_enable" : true,
  "elb_mode" : true
}
```

## Códigos de status

Código de status	Descrição
200	OK
400	Falha na solicitação.
401	O token não tem permissões necessárias.
500	Erro de servidor interno.

## Códigos de erro

Consulte [Códigos de erro](#).



# A Apêndice

## A.1 Código de status

- Normal

Valor retornado	Descrição
200	A solicitação foi processada com sucesso.

- Anormal

Código de status	Estado	Descrição
400	Bad Request	O servidor falha ao processar a solicitação.
401	Unauthorized	A página solicitada requer um nome de usuário e uma senha.
403	Forbidden	O acesso à página solicitada é negado.
404	Not Found	O servidor não consegue encontrar a página solicitada.
405	Method Not Allowed	O método especificado na solicitação não é permitido.
406	Not Acceptable	A resposta gerada pelo servidor não é aceitável para o cliente.
407	Proxy Authentication Required	A autenticação de proxy é necessária antes que a solicitação seja processada.
408	Request Timeout	Um erro de tempo limite ocorre porque a solicitação não é processada dentro do período de espera especificado do servidor.

Código de status	Estado	Descrição
409	Conflict	A solicitação não pode ser processada devido a um conflito.
500	Internal Server Error	A solicitação não é processada devido a um erro do servidor.
501	Not Implemented	A solicitação não é processada porque o servidor não suporta a função solicitada.
502	Bad Gateway	A solicitação não é processada e o servidor recebe uma resposta inválida do servidor upstream.
503	Service Unavailable	A solicitação não é processada devido a uma anormalidade temporária do sistema.
504	Gateway Timeout	Ocorre um erro de tempo limite de gateway.

## A.2 Códigos de erro

Código de status	Códigos de erro	Mensagem de erro	Descrição	Solução
400	WAF.00011001	bad.request	Solicitação inválida	Verificar parâmetro
400	WAF.00011002	url.param.illegal	O formato da URL está incorreto	Verificar formato de URL
400	WAF.00011003	request.body.illegal	Erro de formato do corpo de solicitação: parâmetro ausente e valor ilegal no corpo	Verificar o corpo da solicitação
400	WAF.00011004	id.illegal	ID ilegal	Verificar ID
400	WAF.00011005	name.illegal	Nome ilegal	Verificar nome
400	WAF.00011006	host.illegal	Nome de domínio ilegal	Verificar nome de domínio
400	WAF.00011007	port.illegal	porta ilegal	Verifique a porta
400	WAF.00011007	ip.illegal	IP ilegal	Verificar IP

Código de status	Códigos de erro	Mensagem de erro	Descrição	Solução
400	WAF.00011008	protect.status.illegal	Estatuto de protecção ilegal	Verifique se o estado de proteção está no intervalo de valor de enumeração
400	WAF.00011009	access.status.illegal	Status de acesso ilegal	Verifique se o status de acesso está no intervalo de valor de enumeração
400	WAF.00011010	offsetOrLimit.illegal	Deslocamento ilegal ou número limite	Verifique se a linha de partida ou o número limite está dentro do intervalo
400	WAF.00011011	pageOrPageSize.illegal	Número de página ilegal ou número de entradas por página	Verifique se o número de página ou o número de itens por página estão no intervalo
400	WAF.00011012	standard.violated	Parâmetro inválido	Verifique os parâmetros
400	WAF.00011013	description.illegal	Formato de descrição ilegal	Verificar formato de descrição
400	WAF.00011014	request.header.illegal	Erro no formato do cabeçalho da solicitação: parâmetro ausente e valor ilegal no cabeçalho	Verifique os parâmetros necessários do cabeçalho
400	WAF.00011014	website.not.registered	O site não foi colocado no registro	Arquivamento do site
400	WAF.00012001	invalid.token	Token ilegal	Verifique se o token está correto
400	WAF.00012002	invalid.project	Inconsistência entre project_id e token	Verifique a consistência do project_id e do token
400	WAF.00012003	permission.denied	Sem permissão	Atribuir permissões necessárias do WAF à conta
400	WAF.00012004	account.frozen	Congelamento de conta	Descongelamento da conta

Código de status	Códigos de erro	Mensagem de erro	Descrição	Solução
400	WAF.00012005	not.subscribe	Não subscrito	Inscreeva-se no serviço WAF primeiro
400	WAF.00012006	pdp.permission.denied	Sem permissão	Verifique a autoridade PDP da conta
400	WAF.00012007	jwt.authentication.disabled	Certificação JWT desligada	Abrir certificação JWT
400	WAF.00012008	jwt.authentication.invalid.token	Token JWT ilegal	Verifique se a conta tem permissão JWT
400	WAF.00012009	jwt.authentication.failed	Falha na autenticação JWT	Dê a autorização da conta primeiro
400	WAF.00012010	eps.all.not.support	eps.all.not.support	Abrir a permissão de gravação do projeto empresarial
400	WAF.00013001	insufficient.quota	Quota de função insuficiente	Pacote da elevação da quota da função da compra
400	WAF.00013002	feature.not.support	Função não suportada	nada
400	WAF.00013003	port.not.support	Porta não suportada	Conversão de portas via ELB
400	WAF.00013004	protocol.not.support	Protocolo não suportado	Através do protocolo de conversão ELB
400	WAF.00013005	wildcard.domain.not.support	Nome de domínio Pan não suportado	Usar nomes de domínio específicos
400	WAF.00013006	ipv6.not.support	IPv6 não é suportado	A versão atual não suporta IPv6
400	WAF.00013007	insufficient.tenant.quota	insufficient.tenant.quota	Pacote de atualização de cota de compra
400	WAF.00014001	resource.not.found	Recurso não encontrado	O recurso foi excluído ou não existe
400	WAF.00014002	resource.already.exists	O recurso já existe	O recurso já existe

Código de status	Códigos de erro	Mensagem de erro	Descrição	Solução
400	WAF.00014003	open.protect.failed	Falha ao abrir a proteção	Verificar o status da proteção de nome de domínio
400	WAF.00014004	access.failed	Falha ao acessar o WAF	Modificar resolução de DNS
400	WAF.00014005	bypass.failed	Falha no bypasswaf	Verifique o status da proteção e tente novamente
400	WAF.00014006	proxy.config.error	Erro de configuração do agente	Reconfigure o agente corretamente e tente novamente
400	WAF.00014007	host.conflict	Conflito no nome do domínio	Verifique se o nome de domínio já existe na configuração do site
400	WAF.00014008	cert.inconsistent	O mesmo nome de domínio, mas o certificado é inconsistente	Use o mesmo certificado
400	WAF.00014009	api.not.found	A interface não existe	Verificar o URL da interface
400	WAF.00014010	port.protocol.mismatch	Incompatibilidade de portas e protocolos	Selecione o protocolo e a porta correspondentes
400	WAF.00014011	host.blacklist	É proibido adicionar o site de proteção e o nome de domínio está na lista negra	
400	WAF.00014012	insufficient.tenant.quota	Quota de inquilino insuficiente	Pacote de atualização de cota de compra
400	WAF.00014013	exclusive.ip.config.error	Erro de configuração de IP exclusivo	Verifique a configuração de IP exclusivo
400	WAF.00014014	exclusive.ip.config.error	exclusive.ip.config.error	Verifique a configuração de IP exclusivo

Código de status	Códigos de erro	Mensagem de erro	Descrição	Solução
400	WAF.00021002	url.param.illegal	O formato da URL está incorreto	Recomenda-se modificar a URL no parâmetro do corpo da solicitação para a URL padrão e depurar novamente
400	WAF.00021003	request.body.illegal	O parâmetro solicitado está incorreto	Recomenda-se que você verifique os parâmetros de acordo com o documento antes de iniciar a depuração
400	WAF.00021004	id.illegal	O formato de ID de identificador exclusivo está incorreto	Recomenda-se seguir as instruções corretas na documentação para obter o ID
400	WAF.00021005	name.illegal	O formato do parâmetro name está incorreto	Verifique o formato do nome, que só pode ser composto de letras, números, - e _ e. Não pode exceder 64 caracteres de comprimento
400	WAF.00021006	host.illegal	O formato do nome de domínio está incorreto	Nome de domínio só pode ser composto de letras, números, - e _ e. Não pode exceder 64 caracteres de comprimento
400	WAF.00021007	protocol.illegal	O formato do protocolo back-end está incorreto	O protocolo de back-end só pode ser configurado como HTTP ou HTTPS e deve ser capitalizado
400	WAF.00021008	port.illegal	O formato da porta de origem está incorreto	Verifique se a porta configurada está vazia e se a porta de destino está no intervalo de 0-65535

Código de status	Códigos de erro	Mensagem de erro	Descrição	Solução
400	WAF.00021009	ip.illegal	Formato incorreto de IP	Verifique se o formato IP atende ao formato padrão de IPv4 ou IPv6
400	WAF.00021010	server.address.illegal	Exceção de configuração do servidor	Verifique se a configuração do servidor está vazia e se a quantidade está na faixa de 1-80
400	WAF.00021012	path.illegal	O formato de URL na configuração da regra está incorreto	Recomenda-se modificar a URL no parâmetro do corpo da solicitação para a URL padrão e depurar novamente
400	WAF.00021013	cert.illegal	O certificado HTTPS expirou	Recomenda-se carregar o certificado não expirado novamente
400	WAF.00021014	action.illegal	Ação protetiva ilegal	Recomenda-se configurar ações de proteção de acordo com os valores enumerados no documento
400	WAF.00021015	rule.status.illegal	Status da regra ilegal	Recomenda-se modificar o status da regra de acordo com o valor de enumeração do status da regra no documento
400	WAF.00021016	description.illegal	Exceção Descrição	Recomenda-se usar a gramática inglesa padrão para descrição
400	WAF.00021017	incorrect.rule.config	Configuração incorreta da regra	Recomenda-se configurar as regras de proteção de acordo com a documentação na central de ajuda

Código de status	Códigos de erro	Mensagem de erro	Descrição	Solução
400	WAF.00021018	incorrect.reference.table.config	Configuração incorreta da tabela de referência	Recomenda-se configurar a tabela de referência de acordo com a documentação no centro de ajuda
400	WAF.00021019	incorrect.route.config	Configuração de linha incorreta	Recomenda-se configurar a linha de acordo com a documentação no centro de ajuda
400	WAF.00021020	offsetOrLimit.illegal	Erro de parâmetro de paginação	Recomenda-se preencher os parâmetros de paginação de acordo com os documentos no centro de ajuda
400	WAF.00021021	param.exceed.limit	Parâmetro excede o limite	Recomenda-se visualizar os limites de parâmetros de acordo com a documentação no centro de ajuda
400	WAF.00022002	resource.already.exists	O recurso já existe	Recomenda-se verificar se o recurso criado já existe no console
400	WAF.00022003	resource.is.being.used	O recurso está em uso	Remover a relação entre o recurso e o usuário antes de excluir o recurso
400	WAF.00022004	rule.conflict	Conflito de regras	Verificar se a regra de destino entra em conflito com a regra existente
403	WAF.00022005	insufficient.quota	Recursos insuficientes	Recomenda-se comprar o pacote de atualização dos recursos correspondentes



Código de status	Códigos de erro	Mensagem de erro	Descrição	Solução
404	WAF.00022001	resource.not.found	O recurso não existe	Recomenda-se verificar o status do recurso no console ou solicitar suporte técnico
500	WAF.00010001	internal.error	Erro interno	Entre em contato com o suporte técnico
500	WAF.00010002	system.busy	Erro interno	Entre em contato com o suporte técnico
500	WAF.00010003	cname.failed	Falha ao criar ou modificar CNAME	Entre em contato com o suporte técnico
500	WAF.00010004	cname.failed	Falha ao obter o link de download do arquivo OBS	Entre em contato com o suporte técnico
500	WAF.00020001	internal.error	Exceção interna do serviço	Recomenda-se tentar novamente em cinco minutos
500	WAF.00020002	system.busy	Sistema ocupado	Recomenda-se tentar novamente em cinco minutos

## A.3 Obtenção de ID de projeto

### Obtenção de um ID de projeto chamando uma API

Você pode obter um ID de projeto chamando a API usada para [consultar informações do projeto com base nos critérios especificados](#).

A API usada para obter um ID de projeto é GET `https://{Endpoint}/v3/projects`. **{Endpoint}** é o endpoint do IAM e pode ser obtido em [Regiões e endpoints](#). Para obter detalhes sobre a autenticação da API, consulte [Autenticação](#).

No exemplo a seguir, **id** indica o ID do projeto.

```
{
  "projects": [
    {
      "domain_id": "65382450e8f64ac0870cd180d14e684b",
      "is_domain": false,
      "parent_id": "65382450e8f64ac0870cd180d14e684b",
      "name": "xxxxxxxx",
      "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"
}
}
```

## Obtenção de um ID de projeto no console

Um código de projeto é necessário para alguns URL quando uma API é chamada. Para obter uma ID de projeto, execute as seguintes operações:

1. Acesse o console de gerenciamento.
2. Clique no nome de usuário e escolha **Basic Information** na lista suspensa.
3. Na página **Account Info**, clique em **Manage** ao lado de **Security Credentials**.  
Na página **My Credentials**, visualize os ID de projeto na lista de projetos.

Figura A-1 Visualização dos ID do projeto

