Solution

Building a WAF with Open-Source ModSecurity

Issue	1.0.0
Date	2023-04-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

1 Introduction

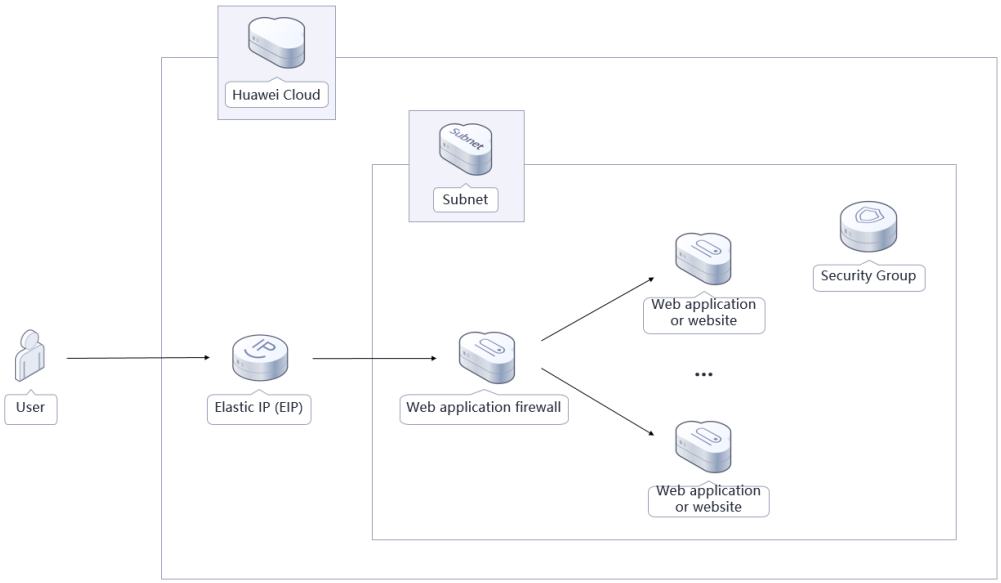
Application Scenarios

This solution helps you deploy a web application firewall (WAF) on Huawei Cloud ECSs in just a few clicks with open-source software ModSecurity. Combining with the flexibility and efficiency of Nginx, this solution can significantly enhance your web security. ModSecurity is an open-source cross-platform web application firewall (WAF). It can protect websites by checking the data received and sent by web servers.

Solution Architecture

This solution uses the open-source ModSecurity software to establish a WAF on Huawei Cloud ECSs. The following figure shows the deployment architecture.

Figure 1-1 Solution architecture



This solution will:

- Create a Linux ECS, which is used for setting up a Web Application Firewall (WAF) and installing Nginx.
- Install and configure Nginx on a Linux ECS to balance workloads.
- Install and configure ModSecurity on a Linux ECS to provide WAF capabilities.
- Create an EIP and bind it to a server so that the server can access the Internet and be accessed from the Internet.

Advantages

- Cost-effectiveness

  Huawei Cloud ECSs provide ultimate performance at competitive prices. You can build a custom WAF on ECSs with open-source ModSecurity.

- Quick deployment

  You can create ECSs and install a WAF on them in just a few clicks.

- Open source and customization

  This solution is open-source and free for commercial use. You can also make custom development based on source code.

Constraints

- Before you start, ensure that you have an account with Huawei Cloud and your account is not in arrears or frozen. You can estimate the total price according to **Table 2-1**.
- Ensure that you have created a VPC, a subnet, a security group, and service ECSs.

2 Resource and Cost Planning

This solution will deploy the resources listed in the following table. The costs are only estimates and may differ from the final prices. For details, see **Pricing Details**.

Table 2-1 Resource and cost planning — ECSs (yearly/monthly)

Huawei Cloud Service	Example Configuration	Estimated Monthly Cost
Elastic Cloud Server (ECS)	• Region: AP-Singapore • Billing Mode: Yearly/Monthly • CPU Architecture: x86 • Type: General computing | s6.medium.2 | 1 vCPU | 2 GB • Image: CentOS 7.6 64bit • System Disk: General Purpose SSD | 100 GiB • Quantity: 1	$29.96 USD
Elastic IP(EIP)	• Region: AP-Singapore • Billing Mode: Yearly/Monthly • Routing Type: Dynamic BGP • Billed By: Bandwidth • Bandwidth: 5 Mbit/s • EIP Quantity: 1	$57.00 USD
Total -		**$86.96 USD**

Table 2-2 Resource and Cost Planning — ECSs (Pay-per-use)

Huawei Cloud Service	Example Configuration	Estimated Monthly Cost
Elastic Cloud Server (ECS)	• Pay-per-use: $0.05 USD/hour • Region: AP-Singapore • Billing Mode: Yearly/Monthly • CPU Architecture: x86 • Type: General computing | s6.medium.2 | 1 vCPU | 2 GB • Image: CentOS 7.6 64bit • System Disk: General Purpose SSD | 100 GiB • Quantity: 1	$0.05 USD* 24 * 30 = $36.0 USD
Elastic IP (EIP)	• Pay-per-use: $0.13 USD/ 5MBit/s/hour • Region: AP-Singapore • Billing Mode: Pay-per-use • Routing Type: Dynamic BGP • Billed By: Bandwidth • Bandwidth: 5 Mbit/s • EIP Quantity: 1	$0.13 USD * 24 * 30 = $93.6 USD
Total -		**$129.6 USD**

3 Procedure

3.1 Preparations

Creating the rf_admin_trust Agency

Step 1 Log in to **Huawei Cloud management console**, move your mouse over the account name, and choose **Identity and Access Management**.

Figure 3-1 Console page

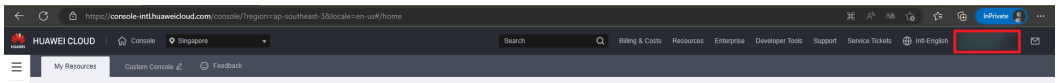
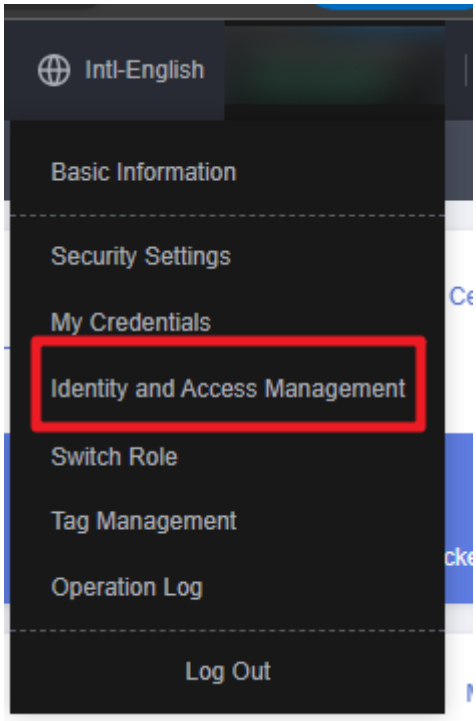
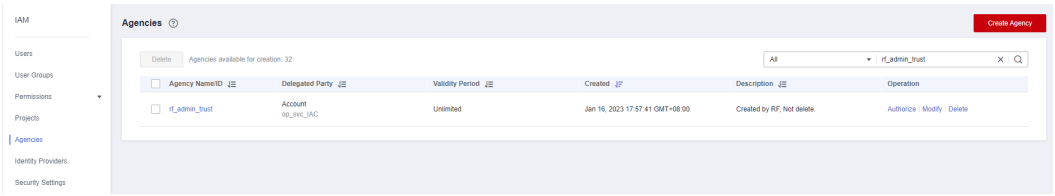


Figure 3-2 Identity and Access Management



Step 2 Choose **Agencies** and then search for the **rf_admin_trust** agency in the agency list.

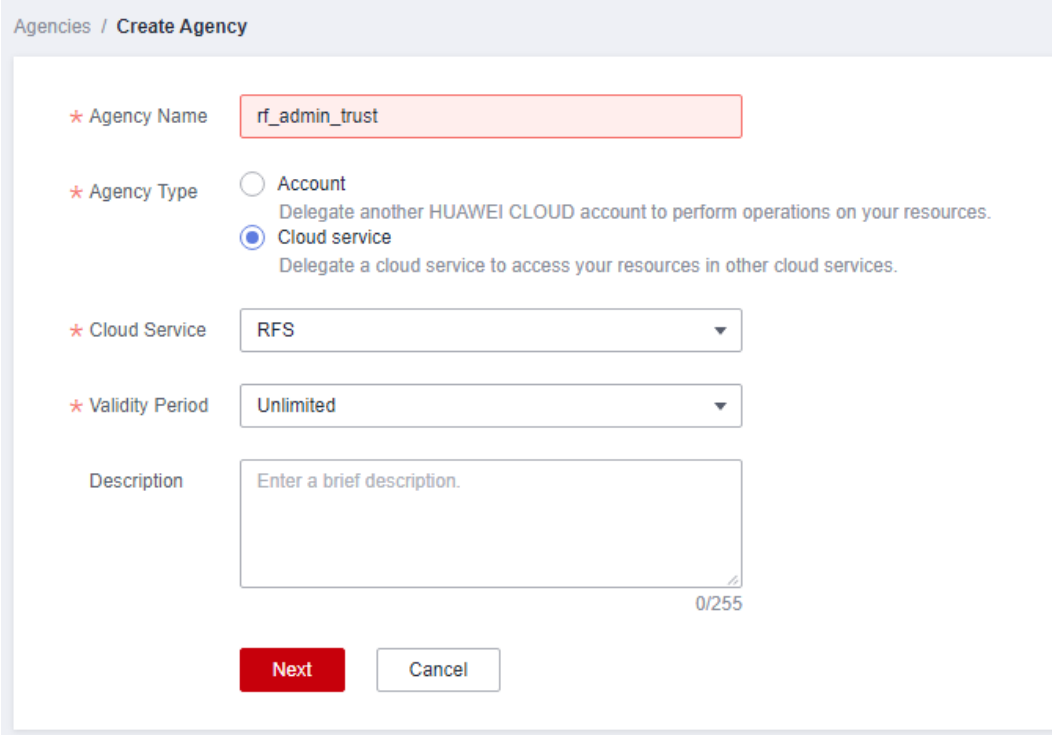
Figure 3-3 Agencies



- If the agency is found, skip the following steps.
- If the agency is not found, perform the following steps to create it.

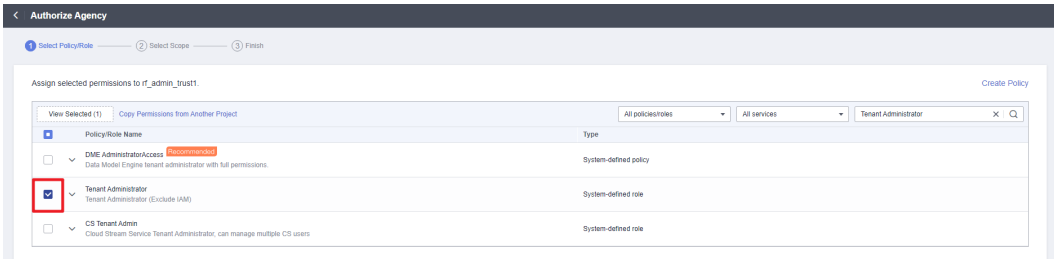
Step 3 Click **Create Agency** in the upper right corner of the page. On the displayed page, enter **rf_admin_trust** for **Agency Name**, select **Cloud service** for **Agency Type**, select **RFS** for **Cloud Service**, and click **Next**.

Figure 3-4 Create Agency



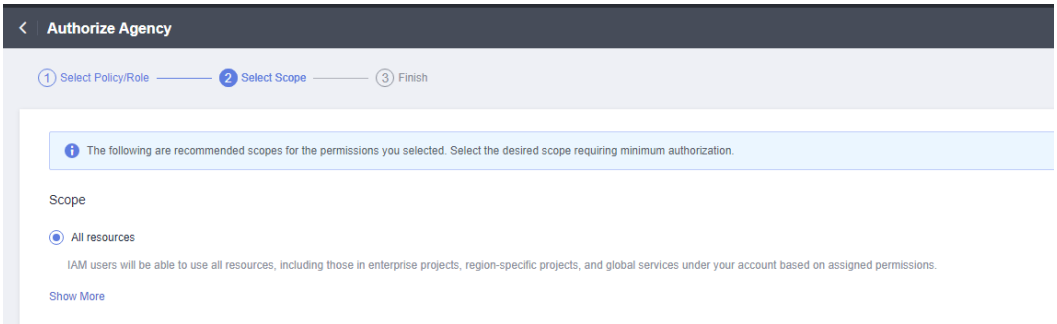
Step 4 Search for **Tenant Administrator** and select it in the search results.

Figure 3-5 Select Policy/Role



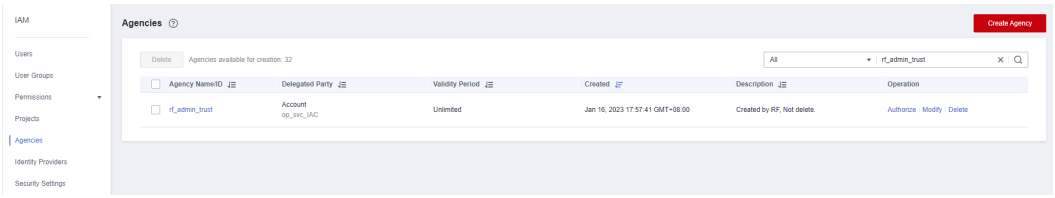
Step 5 Select **All resources** and click **OK**.

Figure 3-6 Select Scope



Step 6 If **rf_admin_trust** is displayed in the agency list, the agency has been created.

Figure 3-7 Agencies

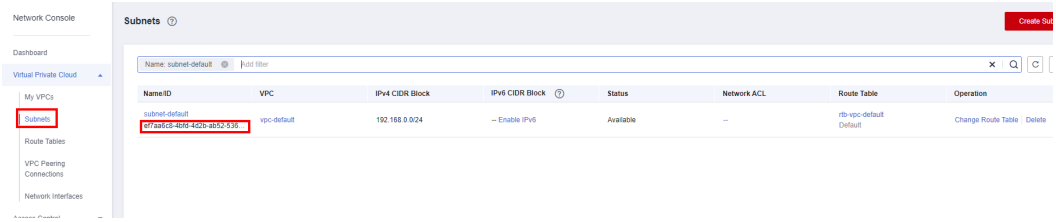


----End

Obtaining the Subnet and Security Group IDs

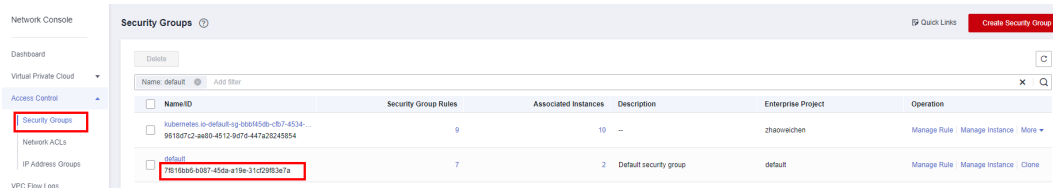
Step 1 Log in to the **Huawei Cloud management console**, go to **the VPC subnet list**, and click the subnet that the backend service servers belong to and obtain the subnet ID.

Figure 3-8 Subnet ID



Step 2 View **the security group list** on the network console, go to the security group configured for the backend service servers, and obtain the security group ID.

Figure 3-9 Security Group ID



----End

3.2 Quick Deployment

This section describes how to quickly deploy this solution.

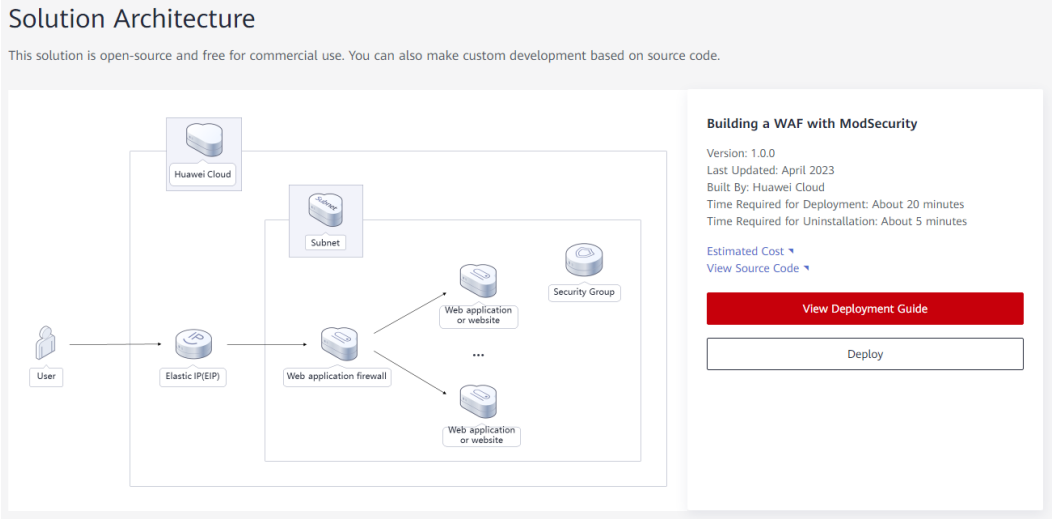
Table 3-1 Parameter description

Parameter	Type	Mandatory	Description	Default Value
subnet_id	String	Yes	Subnet ID. This template uses an existing subnet. Select the subnet in the VPC same as the one your backend service servers belong to. For details, see **Step 1**.	Left blank
security_group_id	String	Yes	Security group ID. This template uses an existing security group. You are advised to select the security group that your backend service servers belong to. For details, see **Step 2**.	Left blank
ecs_name	String	Yes	Name of the ECS for deploying a WAF. The name must be unique. It can contain 1 to 54 characters and can include letters, digits, underscores (_), hyphens (-), and periods (.)	waf_on_modsecurity_demo
ecs_flavor	String	Yes	WAF ECS specifications. For details, see **A Summary List of x86 ECS Specifications**.	s6.medium.2 (1 vCPUs | 2GiB)
ecs_image	String	Yes	WAF ECS image. For more details, see **IMS Public Images**.	CentOS 7.6 64bit.
ecs_password	String	Yes	Initial password of the WAF ECS. After an ECS is created, reset this password by referring to Step 1 in 3.3. The password can include 8 to 26 characters and must include at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters ($!@%-_=+[]:./^,{}?). The password cannot include the username or the username spelled backwards. The administrator username is **root**.	Left blank

Parameter	Type	Mandatory	Description	Default Value
bandwidth_size	Number	Yes	Bandwidth size. This template is billed by bandwidth. Value range: 1 to 2,000 Mbit/s.	5 Mbit/s
ip_list	String	Yes	Private IP address and port for accessing your backend service servers. The format is *IP address 1*:*Port 1*,*IP address 2*:*Port 2*. For example, 192.168.0.1:8080,192.168.0.2:8081,192.168.0.3:8083. (When accessing this environment using a browser, select HTTP or HTTPS based on what the backend port uses.)	Left blank
ssl_certificate	String	Yes	Name of your SSL certificate public key file, including the file name extension. After the template is deployed, upload this certificate file to the **/usr/local/nginx/ssl/** directory on the WAF ECS.	Left blank
ssl_certificate_key	String	Yes	Name of your SSL certificate private key file, including the file name extension. After the template is deployed, upload this certificate file to the **/usr/local/nginx/ssl/** directory on the WAF ECS.	Left blank

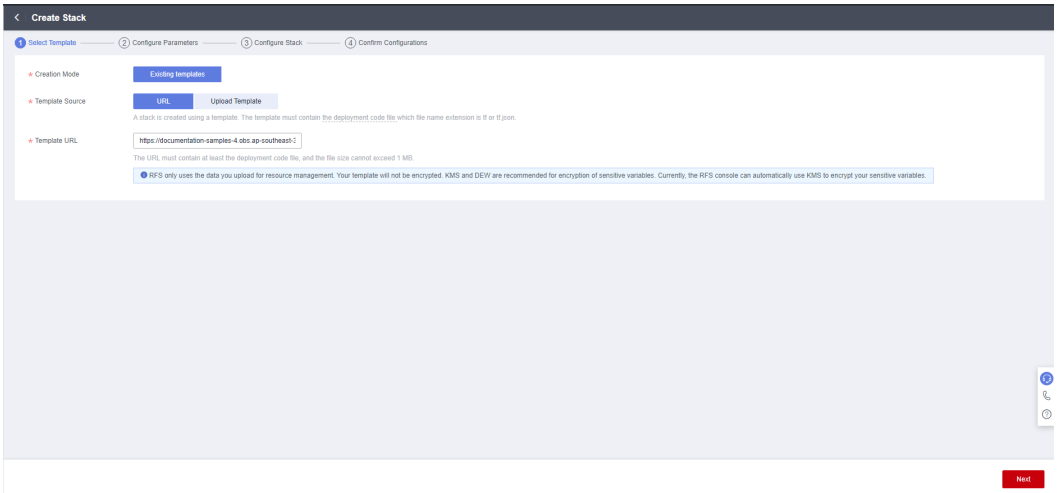
Step 1 Log in to Huawei Cloud Solution Best Practices, choose **Building a WAF with ModSecurity**, and click **Deploy**. The **Create Stack** page is displayed.

Figure 3-10 Selecting a solution



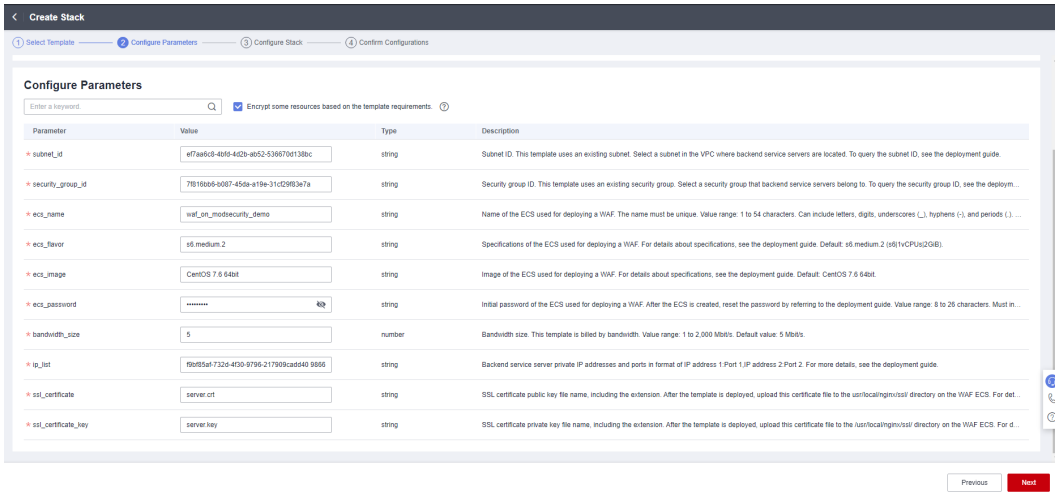
Step 2 On the **Select Template** page, click **Next**.

Figure 3-11 Selecting a template



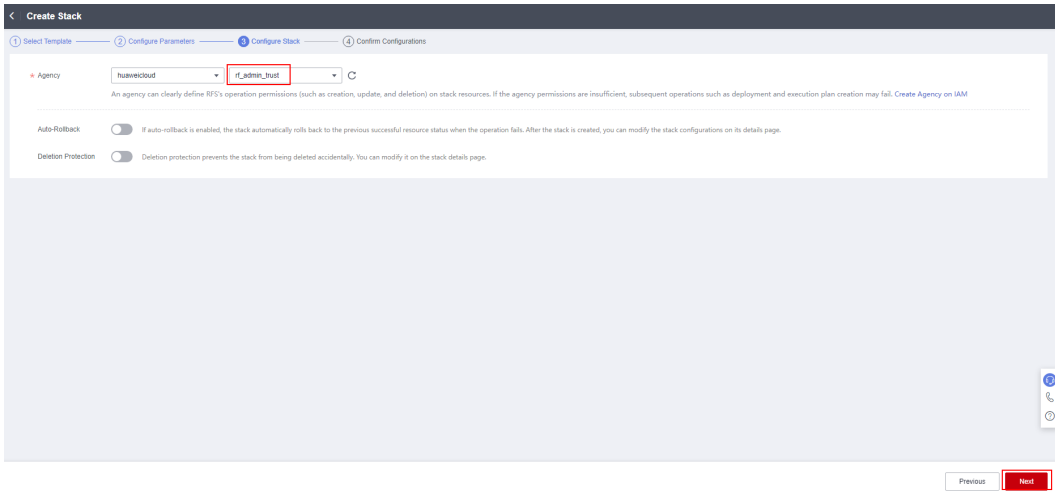
Step 3 On the **Configure Parameters** page, configure parameters by referring to **Table 3-1** and click **Next**.

Figure 3-12 Parameter configuration



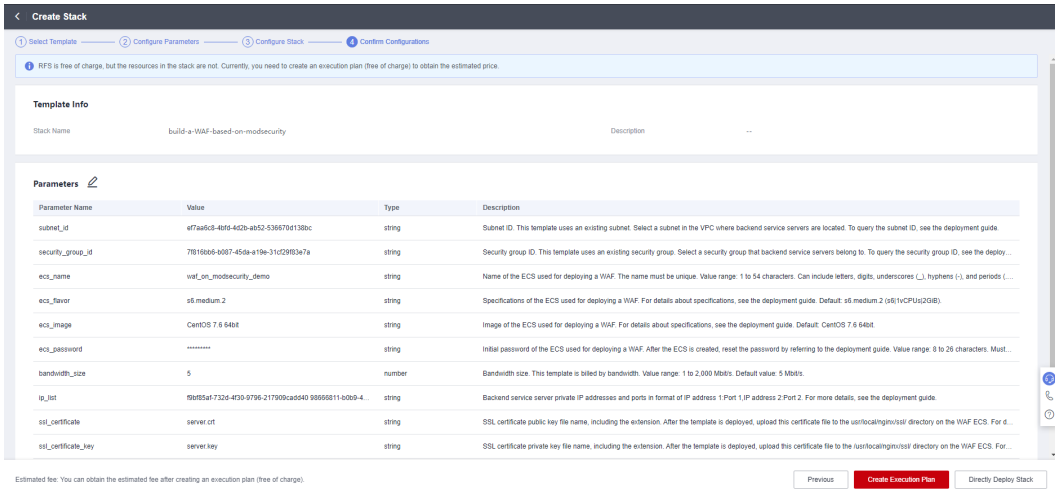
Step 4 On the displayed page, select **rf_admin_trust** from the **Agency** drop-down list and click **Next**.

Figure 3-13 Configure Stack



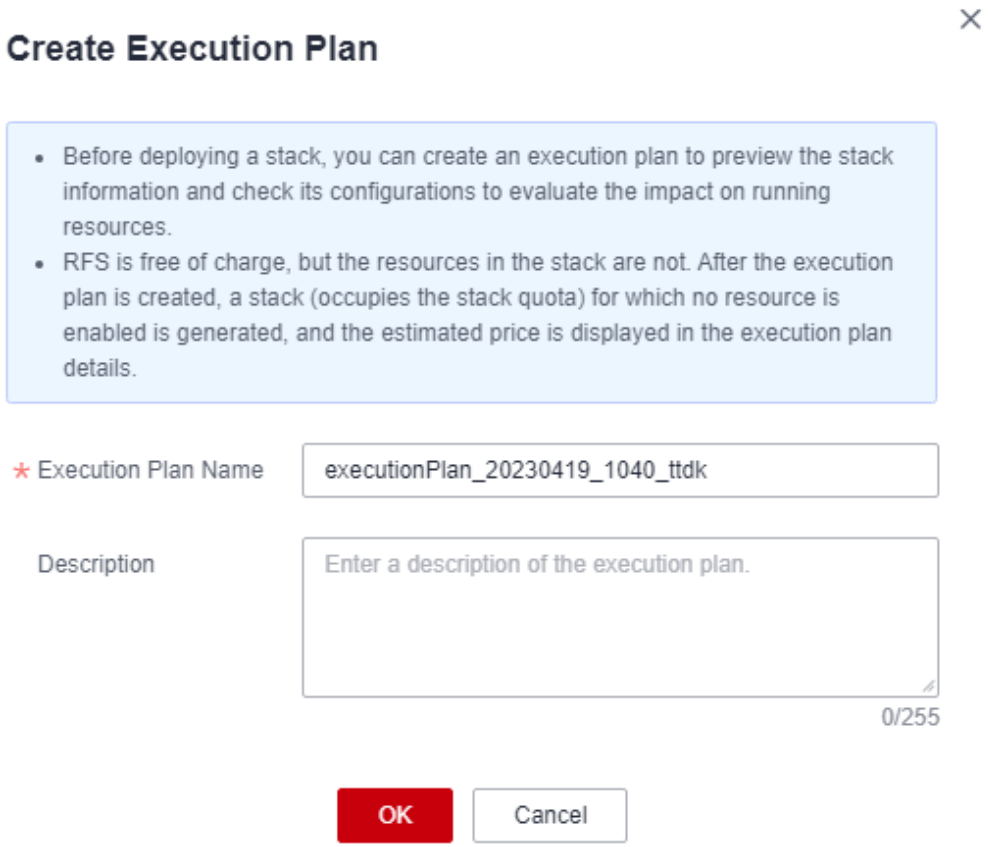
Step 5 On the **Confirm Configurations** page, click **Create Execution Plan**.

Figure 3-14 Confirm Configurations



Step 6 In the displayed **Create Execution Plan** dialog box, enter a plan name and click **OK**.

Figure 3-15 Create Execution Plan



Step 7 Click **Deploy**. In the displayed dialog box, click **Execute**.

Figure 3-16 Execution Plans

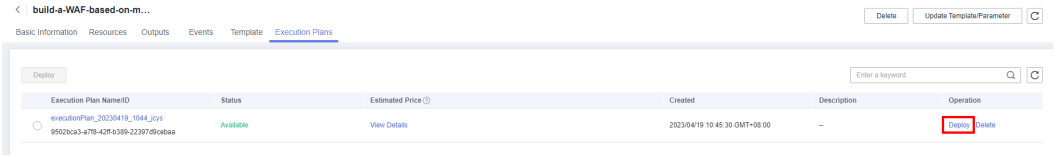
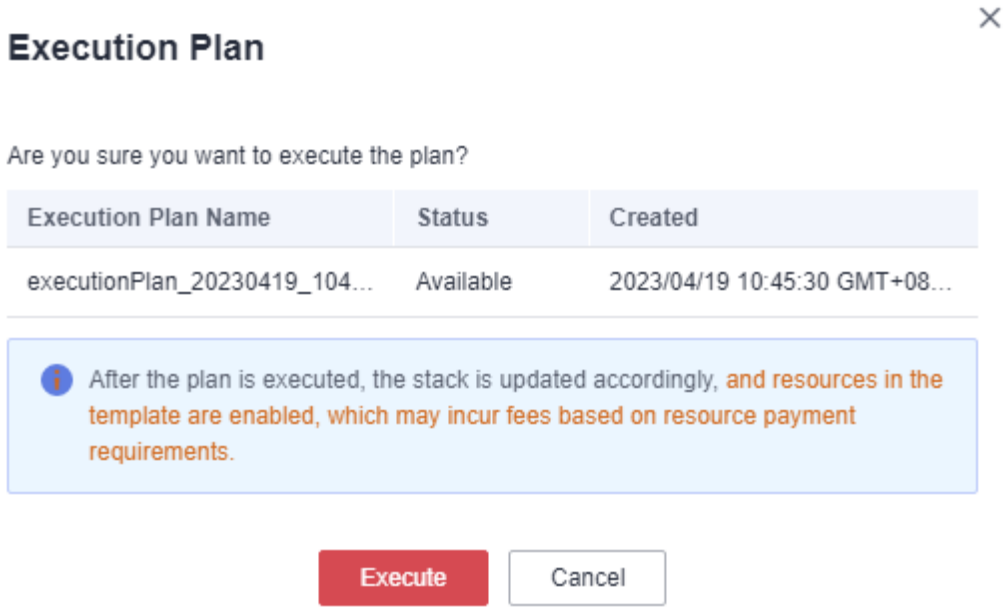
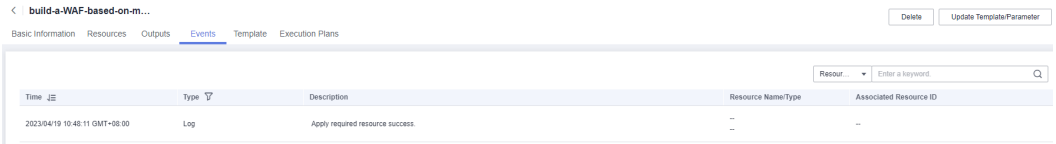


Figure 3-17 Execution Plan



Step 8 Click the **Events** tab and check whether the solution has been deployed. If message "Apply required resource success" is displayed in the **Description** column, the solution has been deployed.

Figure 3-18 Solution deployed



Step 9 Select the **Outputs** tab and obtain the EIP.

Figure 3-19 Obtaining an EIP

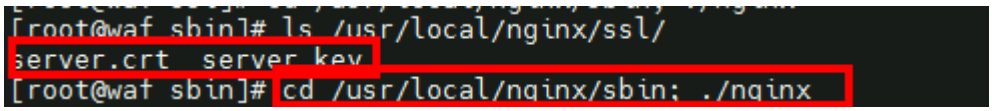
----End

3.3 Getting Started

Step 1 After this solution is deployed, log in to the **ECS console** and reset the password. For details, see **Resetting the Password for Logging In to an ECS on the Management Console**.

Step 2 Use a remote connection tool to log in to the WAF ECS and upload an SSL certificate (public and private key files) to the specified directory: **/usr/local/nginx/ssl/**. For details, see **How Do I Upload Files to My ECS?** Run the **cd /usr/local/nginx/sbin; ./nginx** command to start the Nginx service.

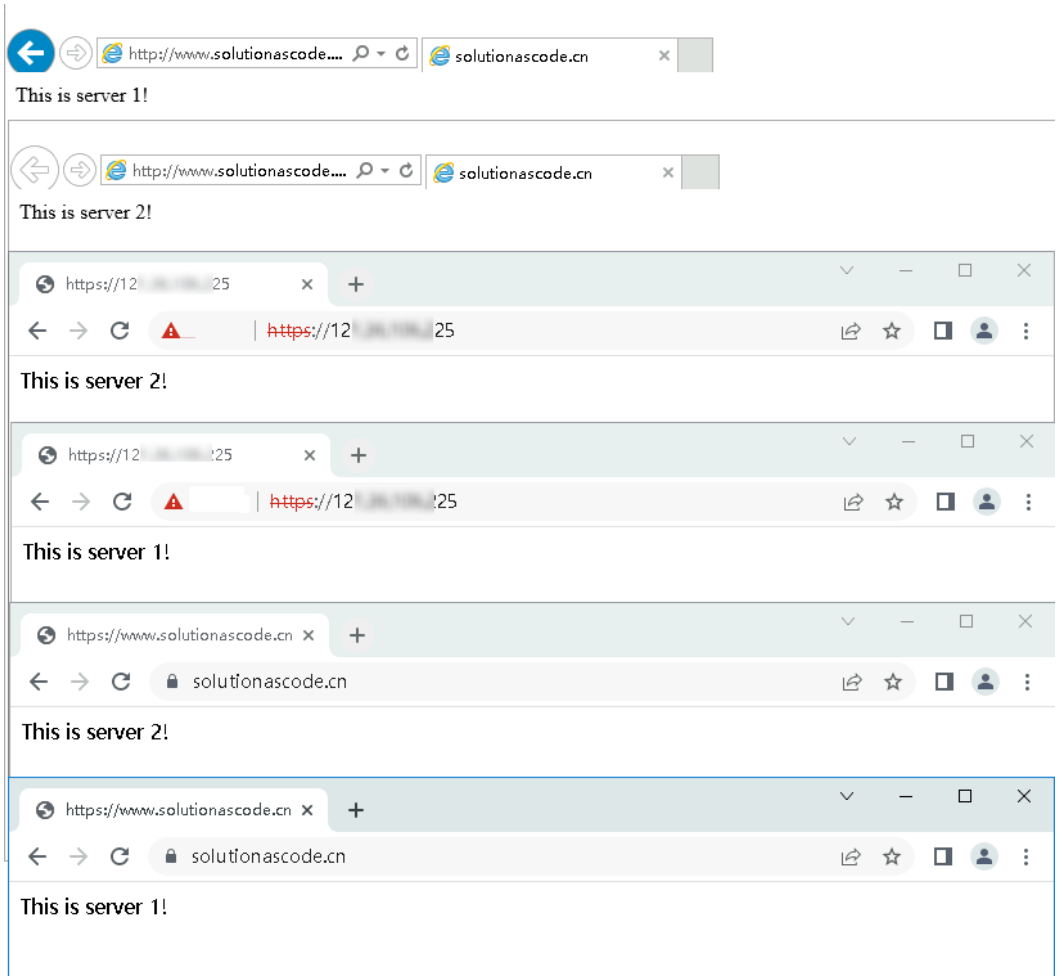
Figure 3-20 Uploading an SSL certificate and starting the Nginx service



Step 3 Configure DNS records. Resolve the website domain name to the EIP obtained in **Step 9**. In this way, the website can be accessed over its domain name. For details about DNS resolution, see **Configuring Record Sets for a Website**.

Step 4 Use a browser to access the EIP or domain name through HTTP/HTTPS many times to verify that requests are distributed across backend service servers. For example, http://EIP, http://Domain name, https://EIP, https://Domain name, or just the domain name.

Figure 3-21 Accessing an EIP mapped to the website private IP address



Step 5 Enter "https://*EIP of the WAF ECS*/?param=%22%3E%3Cscript%3Ealert(1);%3C/script%3E" in the browser address box and check whether WAF takes effect.

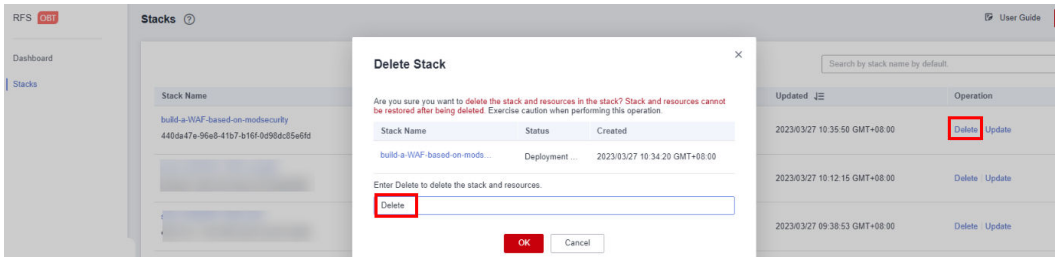
Figure 3-22 Testing WAF

----End

3.4 Quick Uninstallation

Step 1 Log in to **Application Orchestration Service**. On the **Stacks** page, locate the row containing the solution stack you created in **Step 3**, and click **Delete** in the **Operation** column. In the displayed **Delete Stack** dialog box, enter **Delete** in the text box and click **OK**.

Figure 3-23 Delete Stack



----End

4 Appendix

Terms

- **Elastic Cloud Server (ECS)**: ECS provides secure, scalable, on-demand compute resources, enabling you to flexibly deploy applications and workloads.
- **Elastic IP (EIP)**: EIP provides static public IP addresses and scalable bandwidths that enable your cloud resources to communicate with the Internet. You can easily bind an EIP to an ECS, BMS, virtual IP address, NAT gateway, or load balancer, enabling immediate Internet access.
- Nginx: Nginx is a lightweight HTTP server. It is a high-performance HTTP and reverse proxy server as well as an IMAP/POP3/SMTP proxy server. For details, visit **http://nginx.org/en/**.
- ModSecurity is an open-source cross-platform web application firewall (WAF). It can protect websites by checking the data received and sent by web servers. For details, visit **http://www.modsecurity.cn/practice/**.

5 Change History

Released on	Description
2023-04-30	This issue is the first official release.

