Solution

Building a WAF with Open-Source ModSecurity

lssue 1.0.0 Date 2023-04-25





HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.

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

Trademarks and Permissions

NUAWEI 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	1
2 Resource and Cost Planning	3
3 Procedure	5
3.1 Preparations	
3.2 Quick Deployment	
3.3 Getting Started	
3.4 Quick Uninstallation	
4 Appendix	
5 Change History	19

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**.

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

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

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

3_{Procedure}

- 3.1 Preparations
- 3.2 Quick Deployment
- 3.3 Getting Started
- 3.4 Quick Uninstallation

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

IAM	Age	Agencies 🕥									
Users		Delete Agencies available for creat	tion: 32				Al	Ŧ	rf_admin_trust	×Q	
User Groups		Agency Name1D ↓≣	Delegated Party ↓≣	Validity Period ↓≡	Created 4F	Descrip	tion J≣		Operation		
Permissions • Projects		rf_admin_trust	Account op_svc_IAC	Unlimited	Jan 16, 2023 17:57:41 GMT+08:00	Created	by RF, Not delete.		Authorize Modify Delete		
Agencies											
Identity Providers											
Security Settings											

- 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

Agencies / Create Agenci	:y
★ Agency Name	rf_admin_trust
★ Agency Type	 Account Delegate another HUAWEI CLOUD account to perform operations on your resources. Cloud service Delegate a cloud service to access your resources in other cloud services.
* Cloud Service	RFS v
* Validity Period	Unlimited -
Description	Enter a brief description.
	0/255 Next Cancel

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

Figure 3-5 Select Policy/Role

< Authorize Agency							
🚯 Select PaleyRiske (2) Select Scope (3) Fitch							
Assign selected permissions to rf_admin_trust1.	Create Policy						
View Selected (1) Copy Permissions from Another Project	All policies/toles						
Policy/Role Name	Туре						
DRE AdministratorAccess Resourcesson Data Model Engine tenant administrator with full permissions.	System-defined policy						
Tenant Administrator (Exclude IAM)	System-defined role						
CB Tenart Admin Cloud Stream Service Tenant Administrator, can manage multiple CS users	System-defined role						

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

Figure 3-6 Select Scope

<	Authorize Agency
	1 Select Policy/Role 2 Select Scope 3 Finish
	1 The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.
	Scope
	All resources
	AM users will be able to use all resources, including those in enterprise projects, region-specific projects, and global services under your account based on assigned permissions.
	Show More

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

IAM	Agencies ③						Create Agenc
Users	Delete Agencies available	for creation: 32			Al	* rf_admin_trust	X Q
User Groups	Agency NameID ↓≣	Delegated Party ↓≣	Validity Period ↓Ξ	Created 4F	Description J≣	Operation	
Permissions • Projects	rt_admin_trust	Account op_svc_IAC	Unlimited	Jan 16, 2023 17:57:41 GMT+08:00	Created by RF, Not delete.	Authorize Modify Del	lete
Agencies							
Identity Providers							
Security Settings							

----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

Network Console	Subnets ③							Create Sub
Dashboard	Name: subnet-default (Judd filter						× Q C
My VPCs	Name/ID	VPC	IPv4 CIDR Block	IPv6 CIDR Block	Status	Network ACL	Route Table	Operation
Subnets	subnet-default ef7aa6c8-4bfd-4d2b-ab52	-536	192.168.0.0/24	Enable IPv6	Available		rtb-vpc-default Default	Change Route Table Delete
Route Tables								
Connections								
Network Interfaces								

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

Network Console	Security Groups 🕜	curity Groups 💮						
Dashboard	Delete					c		
Virtual Private Cloud 🔹	Name: default 🔘 Add filter					×Q		
Access Control	Name/ID	Security Group Rules	Associated Instances	Description	Enterprise Project	Operation		
Security Groups	bubernetes.io-default-sg-bbb145db-cfb7-4534 9618d7c2-ae80-4512-9d7d-447a28245854	9	10	-	zhaoweichen	Manage Rule Manage Instance More +		
IP Address Groups	default 71816bb6-b087-45da-a19e-31cf29183e7a	7	2	Default security group	default	Manage Rule Manage Instance Clone		
VPC Flow Loos								

----End

3.2 Quick Deployment

This section describes how to quickly deploy this solution.

Table 3-1 Parameter description

Paramete r	Туре	Mandator y	Description	Default Value
subnet_id	StringYesSubnet 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.			
security_gr oup_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_ modsec urity_de mo
ecs_flavor	String	Yes	WAF ECS specifications. For details, see A Summary List of x86 ECS Specifications.	s6.medi um.2 (1 vCPUs 2GiB)
ecs_image	String	Yes	WAF ECS image. For more details, see IMS Public Images.	CentOS 7.6 64bit.
ecs_passw ord	ecs_passw ord String String Yes Initial pa ECS. After reset this referring password character at least t character letters, lo digits, an (\$!@%i password usernam spelled b administ root .		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

Paramete r	Туре	Mandator y	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 <i>IP address 1:Port 1,IP address</i> <i>2.Port 2</i> . For example, 192.168.0.1:8080,192.168.0.2:8 081,192.168.0.3:8083. (When accessing this environment using a browser, select HTTP or HTTPS based on what the backend port uses.)	
ssl_certific ate	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_certific ate_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

olution is op	en-source and free for o	ommercial use. You can also make custom	n development based on source code. Building a WAF with ModSecurity	
	Huawei Cloud		Version: 1.0.0 Last Updated: April 2023	
			Built By: Huawei Cloud	
		and the second second	Time Required for Deployment: About 20 min	utes
		Subast	Time Required for Offinistatiation. About 5 mil	luces
		Sublec	Estimated Cost	
			Security Group	
~		Web applicatio or website	View Deployment Guide	
1	<i></i>			
~			Deploy	
ser	Elastic IP(EIP)	Web application firewall		
		Web application or website	tion	
		or website		

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

Figure 3-11 Selecting a template

< Create Stack		
1 Select Template	- (2) Configure Parameters (3) Configure Stack (4) Configurations	
* Creation Mode	Existing templates	
* Template Source	URL Upload Template A stack is orealised using a template. The template must contain the degloyment code life, which life name extension is if or if juon.	
* Template URL	https://documentation-samples-4-obs.ap-outheast-2	
	The URL must contain at task the deployment cosh tills, and the till ictor control except 1 MI. FIRST only uses the data you upload for resource management. Your template will not be encrypted. XMIS and DEW are recommended for encryption of sensitive variables. Currently, the RFS conside can automatically use XMIS to encrypt your sensitive variables.	
		Next

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

Figure 3-12 Parameter configuration

elect template 🔊 G	Configure Parameters (3) Configure Statick	(a) Contrim Contigurations	
onfigure Parameter	rs		
Enter a keyword.	Q Encrypt some resources based of	on the template requirements.	
Parameter	Value	Туре	Description
subnet_id	el7aa6c8-4bfd-4d2b-ab52-536670d138bc	string	Subnet ID. This template uses an existing subnet. Select a subnet in the VPC where backend service servers are located. To query the subnet ID, see the deployment guide.
security_group_id	71816bb6-b087-45da-a19e-31ct29183e7a	string	Security group ID. This template uses an existing security group. Select a security group that backend service servers belong to. To query the security group ID, see the deploym
ecs_name	waf_on_modsecurity_demo	string	Name of the ECS used for deploying a WAF. The name must be unique. Value range: 1 to 54 characters. Can include letters, digits, underscores (_), hyphens (-), and periods (.)
ecs_flavor	s6.medium.2	string	Specifications of the ECS used for deploying a WAF. For details about specifications, see the deployment guide. Default: s6.medium 2 (x6) tvCPUs(2GIB).
ecs_image	CentOS 7.6 64bit	string	Image of the ECS used for deploying a WAF. For details about specifications, see the deployment guide. Default: CentOS 7.8 64bit.
ecs_password	kQ	string	Initial password of the ECS used for deploying a WAF. After the ECS is created, reset the password by referring to the deployment guide. Value range: 8 to 26 characters. Must in
bandwidth_size	5	number	Bandwidth size. This template is billed by bandwidth. Value range: 1 to 2,000 Mbit's. Default value: 5 Mbit's.
ip_list	f9bf85af-732d-4f30-9796-217909cadd40 9866	string	Backend service server private IP addresses and ports in format of IP address 1 Port 1, IP address 2 Port 2. For more details, see the deployment guide.
ssl_certificate	server.crt	string	SSL certificate public key file name, including the extension. After the template is deployed, upload this certificate file to the usrifocaling/invitsil directory on the WAF ECS. For det
ssl_certificate_key	server.key	string	SSL certificate private key file name, including the extension. After the template is deployed, upload this certificate file to the lusr/local/inginvissl/ directory on the WAF ECS. For d.,

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

Create Stack			
1) Select Template (2) Cor	nfigure Parameters ③ Configure Stack ④ Con	firm Configurations	
RFS is free of charge, but the resolution	urces in the stack are not. Currently, you need to create an execution plan (fre	ae of charge) to obtain the estin	mated price.
Template Info Stack Name	build-a-WAF-based-on-modsecurity		Decaption
Parameters 🖉			
Parameter Name	Value	Туре	Description
subnet_id	el7aa6c8-4bfd-4d2b-ab52-536670d138bc	string	Subnet ID. This template uses an existing subnet. Select a subnet in the VPC where backend service servers are located. To query the subnet ID, see the deployment guide.
security_group_id	71816bb6-b087-45da-a19e-31cf29183e7a	string	Security group ID. This template uses an existing security group. Select a security group that backend service servers belong to. To query the security group ID, see the deploy
ecs_name	waf_on_modsecurity_demo	string	Name of the ECS used for deploying a WAF. The name must be unique. Value range: 1 to 54 characters. Can include letters, digits, underscores (_), hyphens (-), and periods (
ecs_flavor	sõ.medium.2	string	Specifications of the ECS used for deploying a WAF. For details about specifications, see the deployment guide. Default: s6 medium 2 (s6)(wCPUs)2G(B).
ecs_image	CentOS 7.6 64bit	string	Image of the ECS used for deploying a WAF. For details about specifications, see the deployment guide. Default: CentOS 7.6 64bit.
ecs_password		string	Initial password of the ECS used for deploying a WAF. After the ECS is created, reset the password by referring to the deployment guide. Value range: 8 to 26 characters. Must
bandwidth_size	5	number	Bandwidth size. This template is billed by bandwidth. Value range: 1 to 2,000 Mbibs. Default value: 5 Mbibs.
ip_list	19b185a1-732d-4f30-9796-217909cadd40 98656811-b0b9-4	string	Backend service server private IP addresses and ports in format of IP address 1.Port 1,IP address 2.Port 2. For more details, see the deployment guide.
ssl_certificate	server.crt	string	SSL certificate public key file name, including the extension. After the template is deployed, upload this certificate file to the usr/local/nginv/ssl/ directory on the WAF ECS. For d
ssl_certificate_key	server key	string	SSL certificate private key file name, including the extension. After the template is deployed, upload this certificate file to the fushlocalinginuissi' directory on the WAF ECS. For
climited fee: You can obtain the estimate	of fee after coating an exerction plan (fees of channe).		Drawley Presta Eventiles Son Directo Darky Stark

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

Figure 3-15 Create Execution Plan

Create Execution Plan • Before deploying a stack, you can create an execution plan to preview the stack information and check its configurations to evaluate the impact on running resources. • RFS is free of charge, but the resources in the stack are not. After the execution plan is created, a stack (occupies the stack quota) for which no resource is enabled is generated, and the estimated price is displayed in the execution plan details. • Execution Plan Name executionPlan_20230419_1040_ttdk Description Enter a description of the execution plan.

Cancel

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

OK

Figure 3-16 Execution Plans

build-a-WAF-based-on-m Basic Information Resources Outputs Even	is Template Execution Plans			Delete	.date Template/Parameter
Deploy				Enter a keyword.	QC
Execution Plan Name/ID	Status	Estimated Price ()	Created	Description	Operation
executionPlan_20230419_1044_jcys 9502bca3-a718-42ff-b389-2239749cebaa	Available	View Datails	2023/04/19 10:45:30 GMT+08:00		Deploy Delete

Figure 3-17 Execution Plan

Execution Plan Status Created execution Plan Name Status Created executionPlan_20230419_104... Available 2023/04/19 10:45:30 GMT+08... Image: After the plan is executed, the stack is updated accordingly, and resources in the template are enabled, which may incur fees based on resource payment requirements. Execute Cancel

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

< build-a-WAF-based-on-m					Delete	Update Template/Parameter
Basic Information Resources Outputs	Events Template Exec	ution Plans				
				Resour +	Enter a keyword.	Q
Time J≣	Туре 🔽	Description	Resource Name/Type	Ass	ciated Resource ID	
2023/04/19 10:48:11 GMT+08:00	Log	Apply required resource success.		-		

Step 9 Select the Outputs tab and obtain the EIP.

Figure 3-19 Obtaining an EIP

<	build-a-WAF-based-on-m	Townline Discussion Discus		A The state ID address of the WAT is		Delete	Update Template/Parameter
	sic mormanon resources Oupors evens	rempiare execution Plans		 The public in adults's of the type is 190 92:190 222, You can use this IP to access web servers from your browser. 2. After the template is deployed, upload SSL certificate public and private key files to the 		Enter a keyword.	Q C
	Name	Туре	Value	/usr/local/nginx/ssi/ directory.	Description		
	说明	string	1. The publ	c IP address of the WAF is 190.92.199.222. You can use this IP to	-		

⁻⁻⁻⁻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

[root@waf_sbin]# ls_/usr/local/nginx/ssl/ server.crt_server_key [root@waf_sbin]#_cd_/usr/local/nginx/sbin; ./nginx______

- 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.



----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.