solution

Building a Remote O&M Environment with JumpServer

Issue 1.0

Date 2024-04-22

HUAWEI

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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Solution Overview

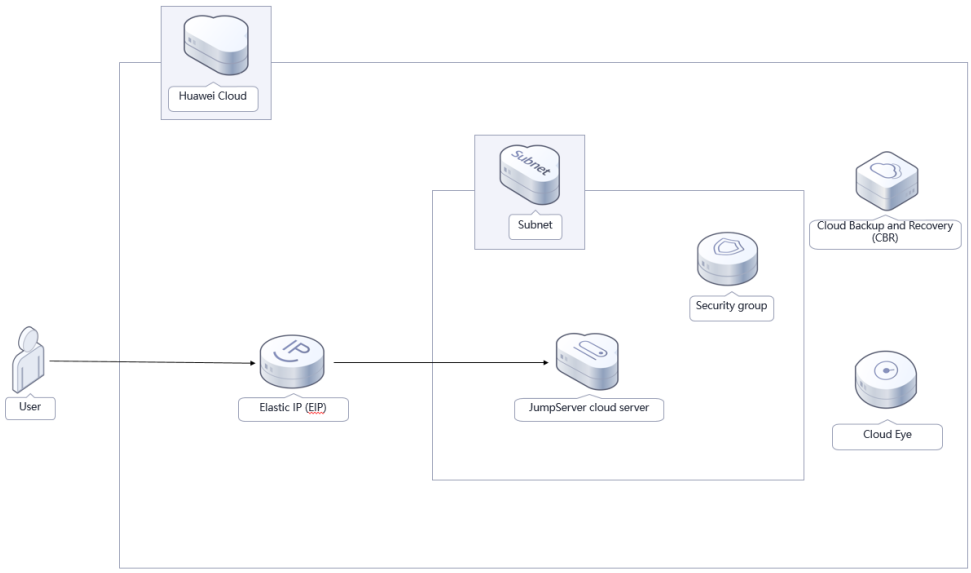
Scenarios

This solution helps you quickly set up a remote secure O&M environment with JumpServer on Huawei Cloud Elastic Cloud Servers (ECSs). It provides an efficient, reliable, and secure way for enterprises to manage infrastructure and applications. This solution can be used in sectors such as finance, manufacturing, service, and Internet. It is suitable for a range of scenarios that require server security control.

Solution Architecture

You can use this solution to deploy a remote secure O&M environment with JumpServer on Huawei Cloud ECSs, in just a few clicks. The following figure shows the solution architecture.

Figure 1-1 Architecture



This solution will:

- Create a Linux ECS for installing JumpServer to set up a secure remote O&M environment.
- Create an EIP and bind it to an ECS for Internet access.
- Create security groups with specified rules to control traffic to and from ECSs.

In addition, you can use Cloud Eye to monitor the ECS status and purchase Cloud Backup and Recovery (CBR) to back up ECS data.

Advantages

- High security

  This solution adopts a multi-layer security protection system with security measures such as role-based access control, audit logs, and multi-factor authentication to prevent malicious attacks and improper operations from internal personnel.

- Effective management

  This solution provides comprehensive management functions, covering user management, asset management, account management, and permissions management. These functions facilitate user management and monitoring, ensuring system stability and reliability.

- Easy deployment

  In just a few clicks, you can easily create ECSs and EIPs and install the JumpServer bastion host system.

Constraints

- Before deploying this solution, register a HUAWEI ID, enable Huawei Cloud services, and complete real-name authentication. If you select the yearly/monthly billing mode, ensure that your account has sufficient balance. If you do not have sufficient balance, you can go to the Billing Center to manually pay for the order.
- If you want to use IAM agencies to deploy resources, ensure that your HUAWEI ID has sufficient IAM permissions. For details, see **(Optional) Creating the rf_admin_trust Agency**. If you use an account (HUAWEI ID) or you use an IAM user in the admin user group, you do not need to select an agency, and the solution will be deployed based on the permissions of the login user.

2 Resource Planning and Costs

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 **Huawei Cloud Pricing**.

Table 2-1 Resource planning and costs (yearly/monthly)

Huawei Cloud Service	Example Configuration	Estimated Monthly Cost
Elastic Cloud Server (ECS)	• Region: AP-Singapore • Billing Mode: Yearly/Monthly • Type: x86 | General computing | s6.xlarge.2 | 4vCPUs | 8GB • Image: CentOS 7.9 64bit • System Disk: High I/O | 100GB • Quantity: 1	$76.93 USD
Elastic IP (EIP)	• Pay-per-use: $0.12 USD/EIP/GB • Region: AP-Singapore • Billing Mode: Pay-per-use • Product Type: Dedicated • Routing Type: Dynamic BGP • Billed By: Traffic • EIP Quantity: 1	$0.12 USD/GB
Total		$76.93 USD + EIP price

Table 2-2 Resource planning and costs (pay-per-use)

Huawei Cloud Service	Example Configuration	Estimated Monthly Cost
Elastic Cloud Server (ECS)	• Pay-per-use: $0.15 USD/ECS/hour • Region: AP-Singapore • Billing Mode: Pay-per-use • Type: x86 | General computing | s6.xlarge.2 | 4vCPUs | 8GB • Image: CentOS 7.6 64bit • System Disk: High I/O | 100GB • Required Duration: 1 month • Quantity: 1	$100.80 USD
Elastic IP (EIP)	• Pay-per-use: $0.12 USD/EIP/GB • Region: AP-Singapore • Billing Mode: Pay-per-use • Product Type: Dedicated • Routing Type: Dynamic BGP • Billed By: Traffic • EIP Quantity: 1	$0.12 USD/GB
Total		$100.80 USD + EIP price

3 Procedure

3.1 Preparations

(Optional) Creating the rf_admin_trust Agency

Step 1 Log in to the **Huawei Cloud console**, hover your mouse over the account name in the upper right corner, and choose **Identity and Access Management**.

Figure 3-1 Huawei Cloud console

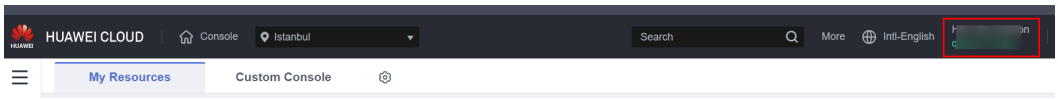
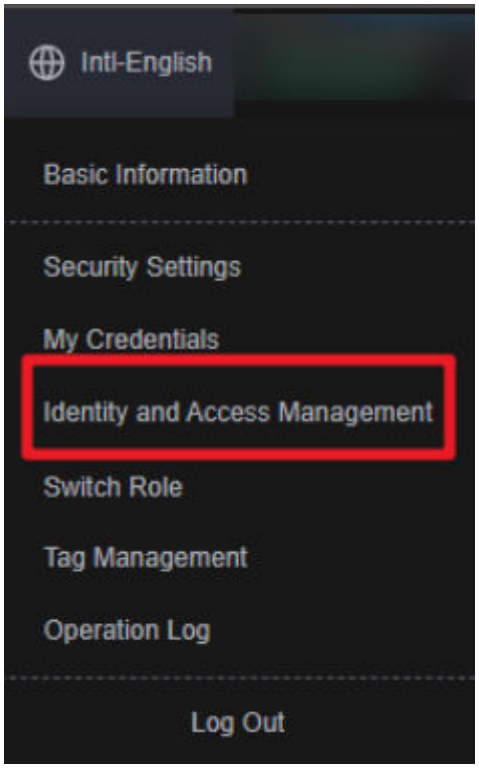
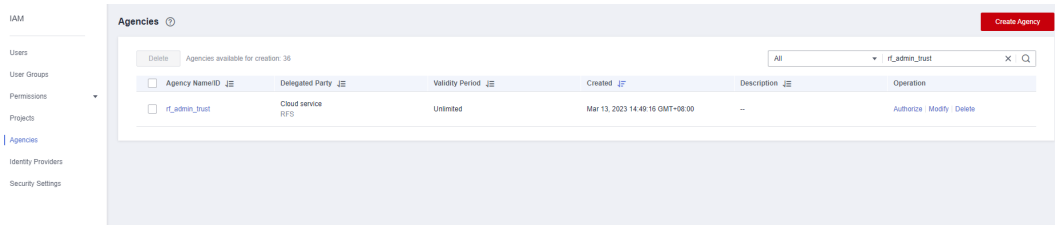


Figure 3-2 Identity and Access Management



Step 2 Choose **Agencies** in the navigation pane and search for the **rf_admin_trust** agency.

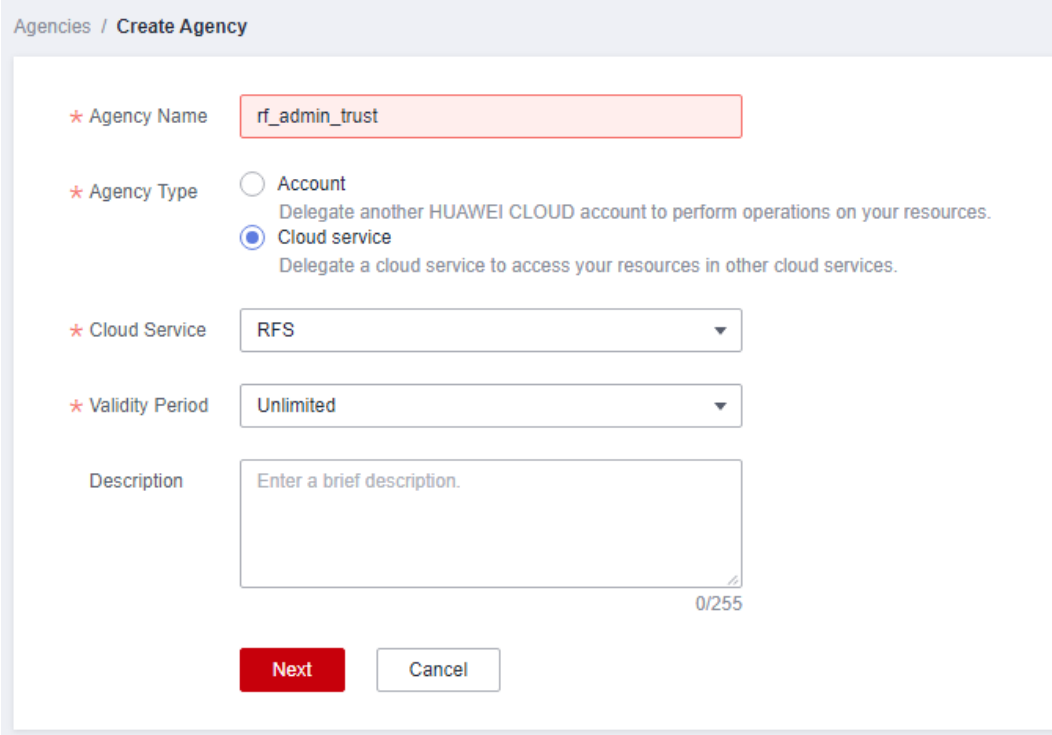
Figure 3-3 Agency list



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

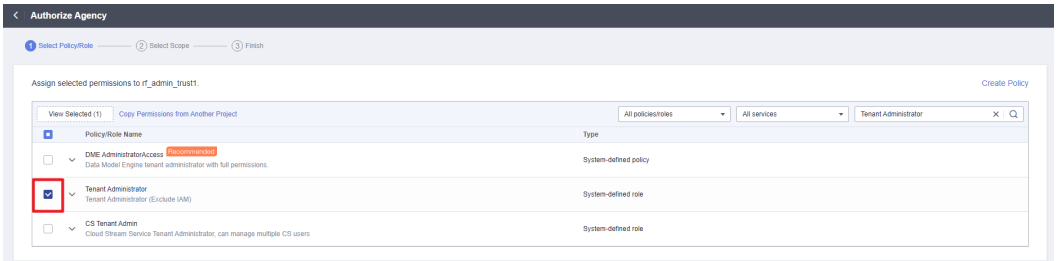
Step 3 Click **Create Agency** in the upper right corner of the page. On the displayed page, set **Agency Name** to **rf_admin_trust**, **Agency Type** to **Cloud service**, **Cloud Service** to **RFS**, and click **Next**.

Figure 3-4 Creating an agency



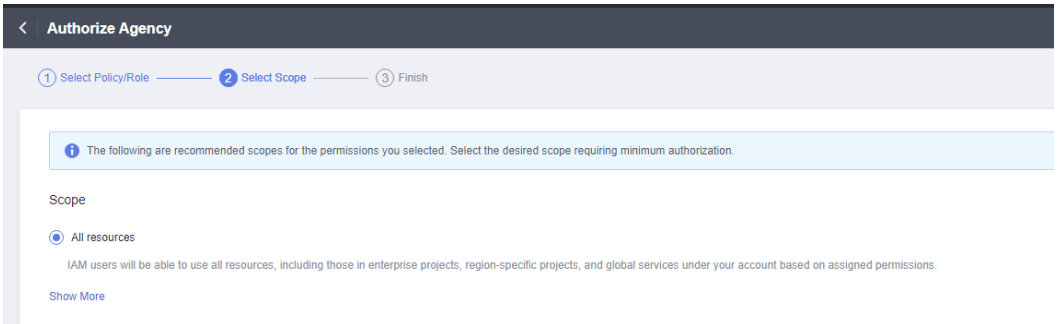
Step 4 Search for **Tenant Administrator**, select it in the search results, and click **Next**.

Figure 3-5 Selecting a policy



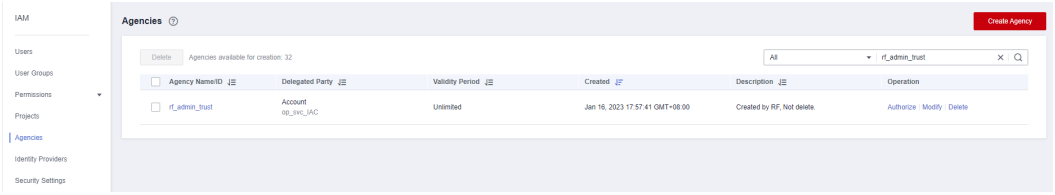
Step 5 Select **All resources** and click **OK**.

Figure 3-6 Selecting the authorization scope



Step 6 Check that the **rf_admin_trust** agency is displayed in the agency list.

Figure 3-7 Agency list



----End

3.2 Quick Deployment

This section describes how to quickly deploy this solution.

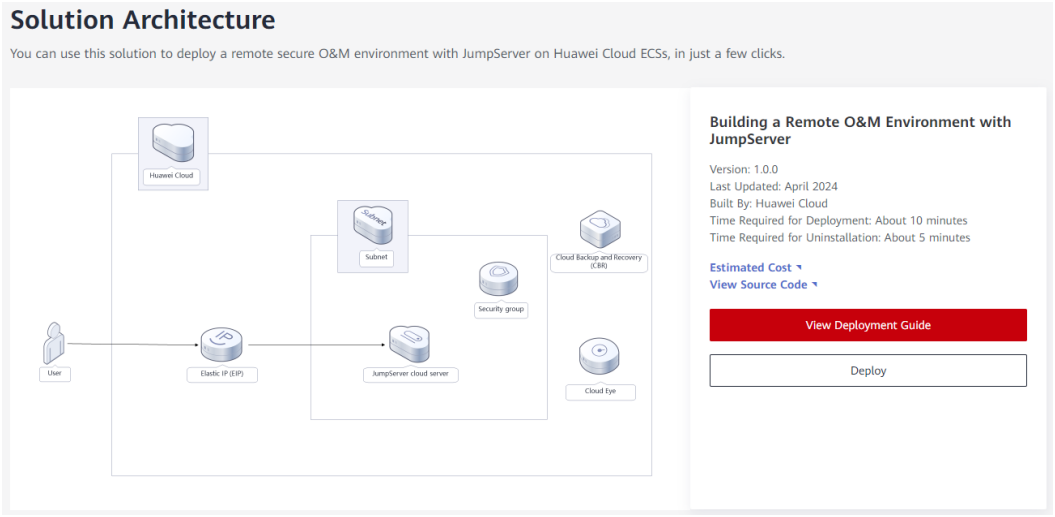
Table 3-1 Parameter description

Parameter	Type	Mandatory	Description	Default Value
vpc_name	String	Yes	Virtual Private Cloud (VPC) name. This template uses a newly created VPC. The VPC name must be unique. It can contain 1 to 54 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.	remote-OM-environment-with-jumpserver-demo
secgroup_name	String	Yes	Security group name. This template uses a newly created security group. For details about how to configure a security group rule, see **(Optional) Modifying Security Group Rules**. It can contain 1 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.	remote-OM-environment-with-jumpserver-demo
ecs_name	String	Yes	ECS name. It must be unique. It can contain 1 to 60 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.	remote-OM-environment-with-jumpserver-demo
ecs_flavor	String	Yes	ECS flavor. For more flavors, see **A Summary List of x86 ECS Specifications**.	s6.xlarge.2

Parameter	Type	Mandatory	Description	Default Value
ecs_password	String	Yes	Initial password of an ECS. It can contain 8 to 26 characters and must include at least three of the following character types: uppercase letters, lowercase letters, digits, and the following special characters (!@$%^-_=+[{()}]:,./?~#*). For Windows ECSs, the password cannot contain the username, the username spelled backwards, or more than two consecutive characters in the username. The default administrator account is **root**.	Left blank
ecs_disk_size	Number	Yes	ECS system disk size, in GB. The default disk type is high I/O. The disk size cannot be decreased. Value range: 40-1,024	100
bandwidth_size	Number	Yes	EIP bandwidth size, in Mbit/s. EIPs are billed by traffic. Value range: 1-300	300
charging_mode	String	Yes	Billing mode. It can be **prePaid** (yearly/monthly) or **postPaid** (pay-per-use).	postPaid
charging_unit	String	Yes	Unit of an ECS subscription term. This parameter is only mandatory if **charging_mode** is set to **prePaid**. Value range: **month** or **year**	month
charging_period	Number	Yes	ECS subscription term. This parameter is only mandatory if **charging_mode** is set to **prePaid**. Value range: • 1-9 (**charging_unit** set to **month**) • 1-3 (**charging_unit** set to **year**) The default subscription term is one month.	1

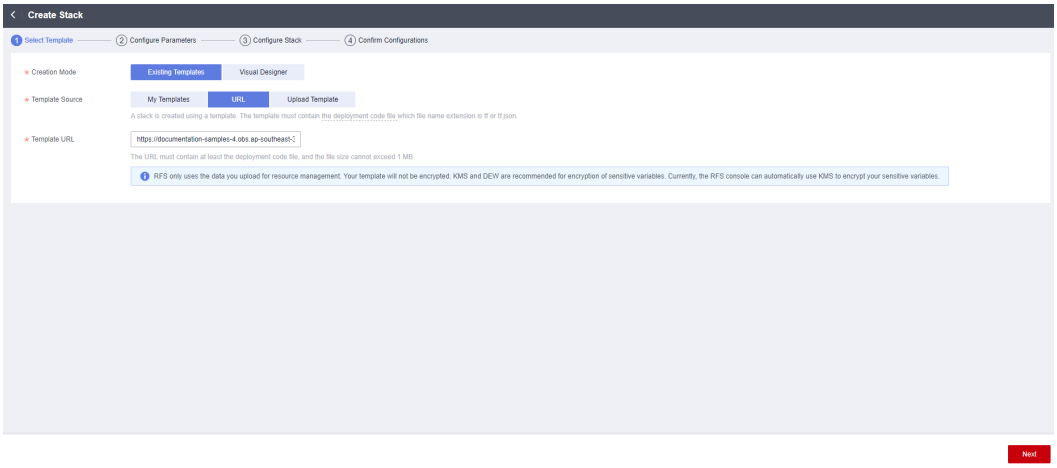
Step 1 Access Huawei Cloud **Quick-Start Guides** and choose **Building a Remote O&M Environment with JumpServer**. Click **Deploy** to switch to the **Create Stack** page.

Figure 3-8 Selecting a solution



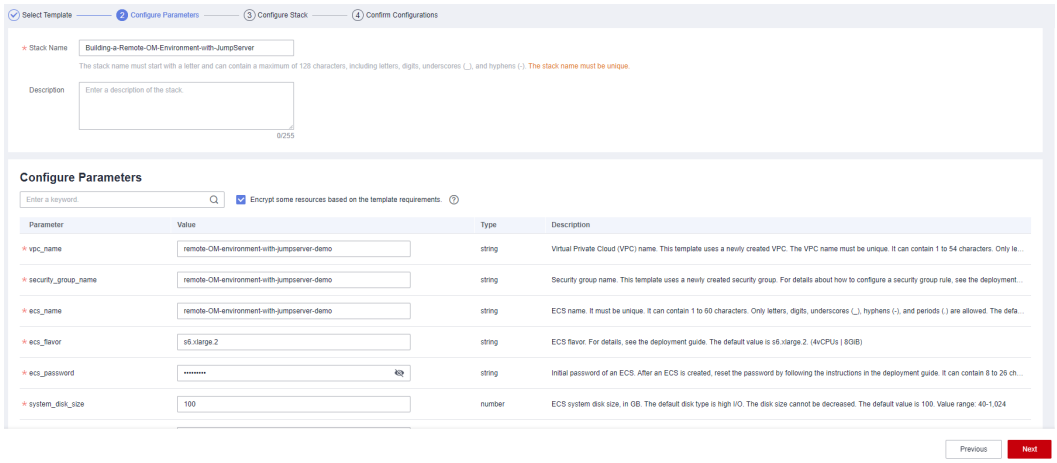
Step 2 On the **Select Template** page, select a template and click **Next**.

Figure 3-9 Selecting a template



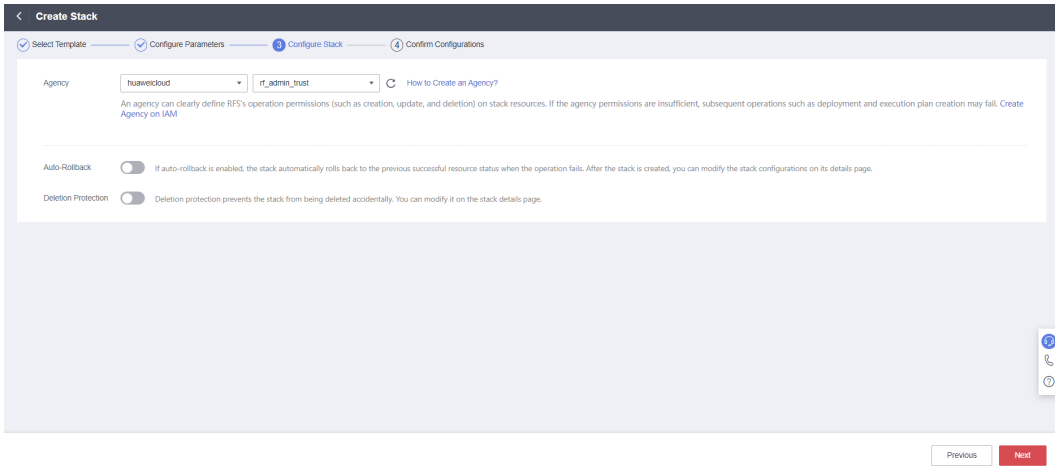
Step 3 On the **Configure Parameters** page, configure parameters based on **Table 3-1**, and click **Next**.

Figure 3-10 Configuring parameters



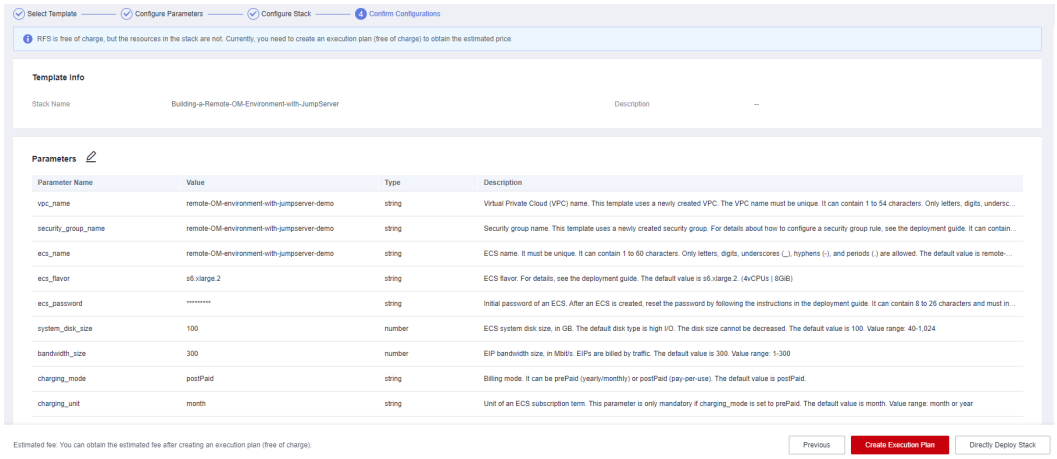
Step 4 On the **Configure Stack** page, select **rf_admin_trust** from the **Agency** drop-down list and click **Next**. This step is optional if you use an account (HUAWEI ID) or use an IAM user in the **admin** user group.

Figure 3-11 Configuring a stack



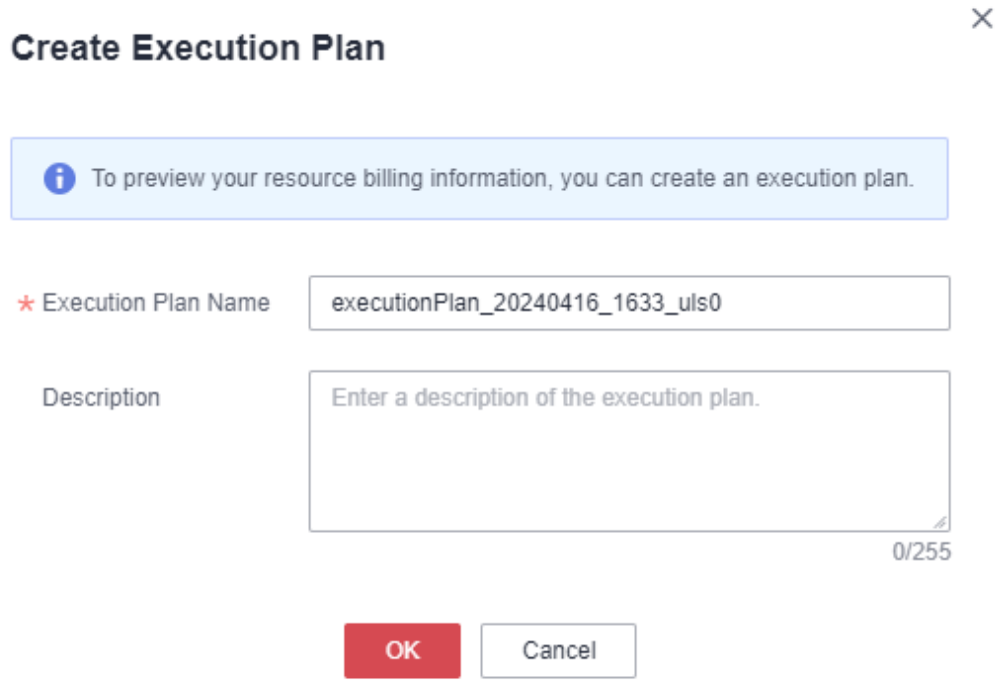
Step 5 On the **Confirm Configurations** page, confirm the configurations and click **Create Execution Plan**.

Figure 3-12 Confirming configurations



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

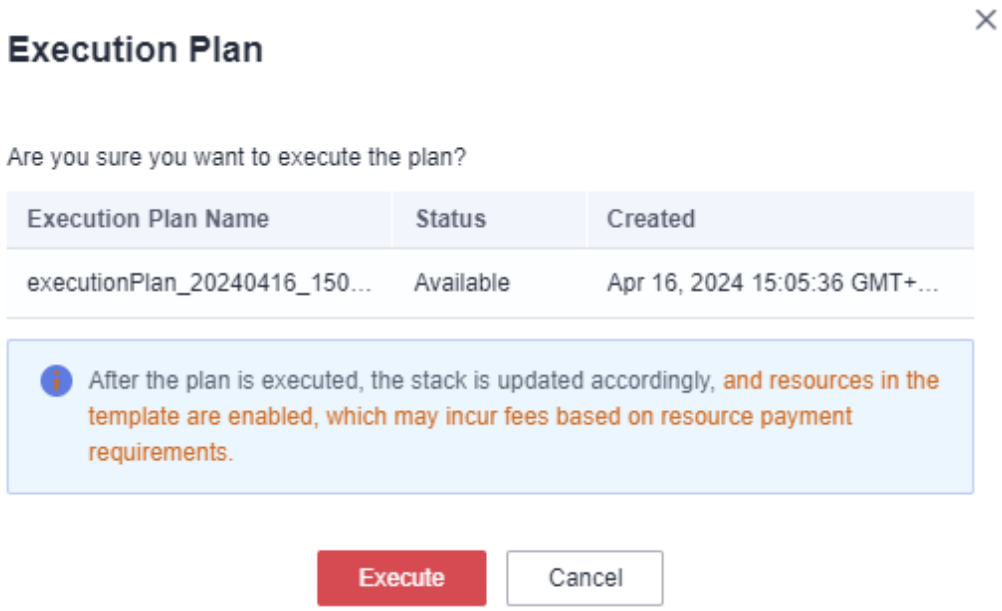
Figure 3-13 Creating an execution plan



Step 7 Wait until the status of the execution plan changes to **Available**, and then click **Deploy** in the **Operation** column. In the displayed dialog box, click **Execute**.

Figure 3-14 An execution plan created

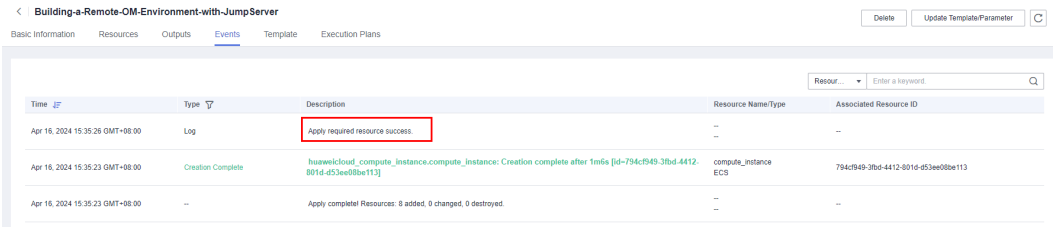
Figure 3-15 Confirming the execution plan



Step 8 (Optional) If you select the yearly/monthly billing mode and your account balance is insufficient, log in to the Billing Center to manually pay for the order. You can refer to **Table 2-1** to see the total price.

Step 9 Wait until the deployment completes and click the **Events** tab to view details.

Figure 3-16 Resources created



Step 10 Refresh the page to view the JumpServer access description on the **Outputs** tab.

Figure 3-17 Access description

----End

3.3 Getting Started

(Optional) Modifying Security Group Rules

A security group is a collection of access control rules to control traffic to and from cloud resources, such as cloud servers, containers, and databases. Cloud resources associated with the same security group have the same security requirements and are mutually trusted within a VPC.

You can modify security group rules, for example, by adding, modifying, or deleting a TCP port, as follows:

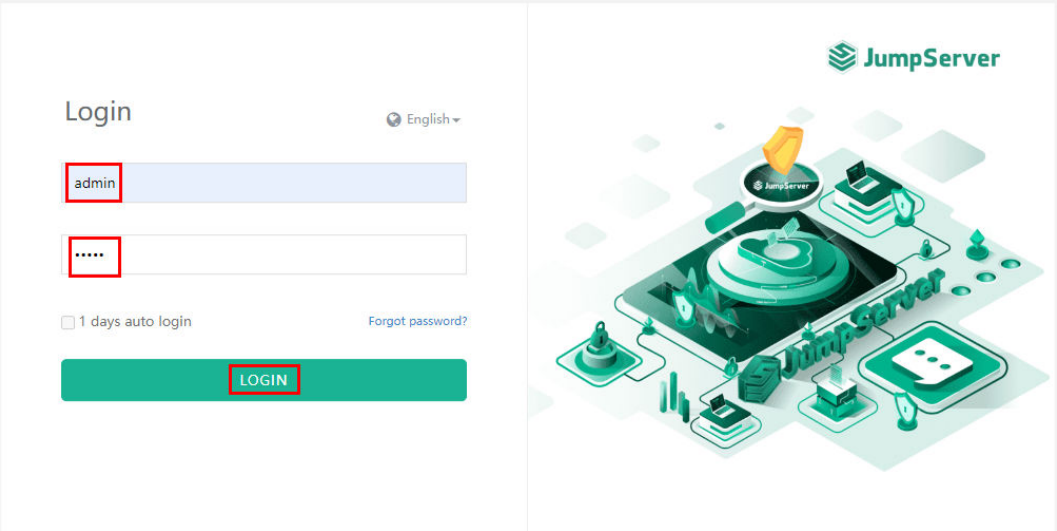
- Adding a security group rule: **Add an inbound rule** and enable a TCP port if needed.
- Modifying a security group rule: Inappropriate security group settings may introduce serious security risks. You can **modify security group rules** to ensure the network security of your ECSs.
- Deleting a security group rule: If the source or destination IP address of an inbound or outbound security group rule changes, or a port needs to be disabled, you can **delete the security group rule**.

NOTICE

If default parameter settings are retained, the initial solution deployment takes about 10 minutes. The time required for deployment varies depending on factors such as ECS flavors and EIP bandwidth.

Step 1 Log in to JumpServer. Open the browser and enter the URL in **step 10 in "Quick Deploy...**. The JumpServer login page is displayed. Enter the username and password and click **LOGIN**. (The initial username and password are **admin**.)

Figure 3-18 Login page



Step 2 Reset the password and access the management console. Follow the instructions to enter and confirm the new password. Then, click **Setting** and use the new password to access the JumpServer console.

Figure 3-19 Resetting the password

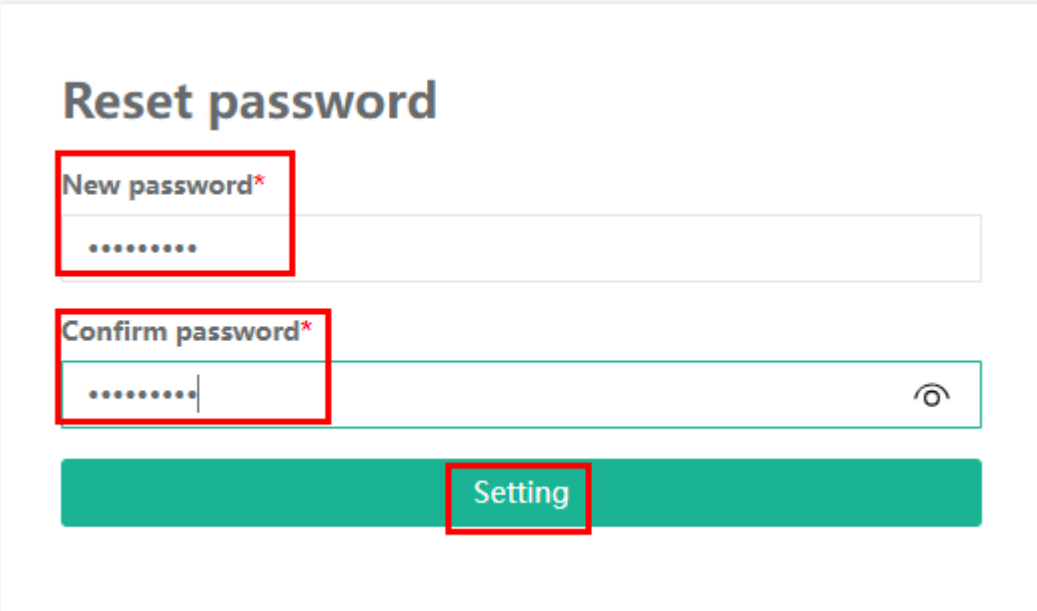
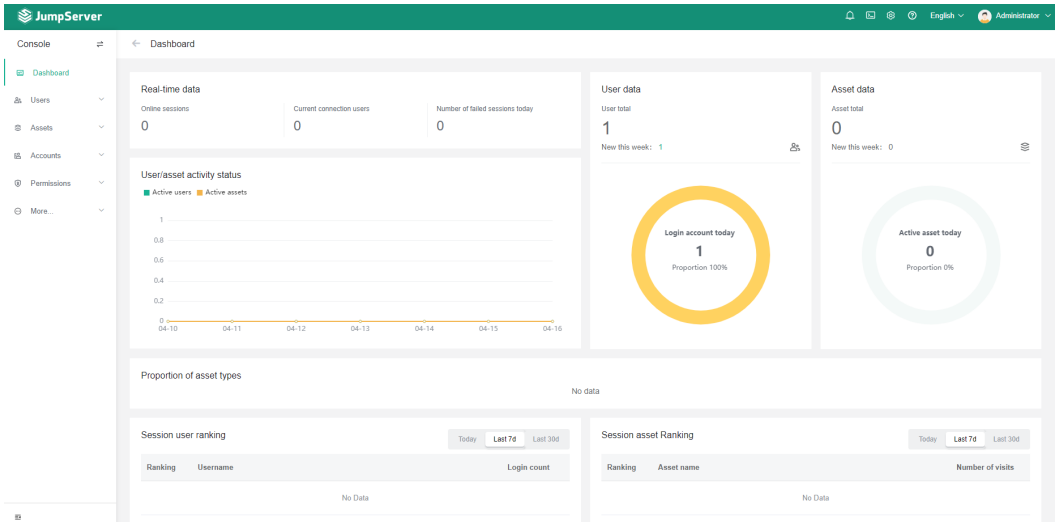
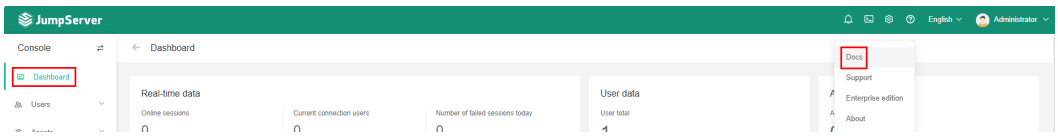


Figure 3-20 JumpServer console



Step 3 Access JumpServer documentation. Hover your mouse over the position marked in the upper right corner and click **Docs**. The JumpServer documentation page is displayed for you to learn more about JumpServer.

Figure 3-21 Viewing documentation

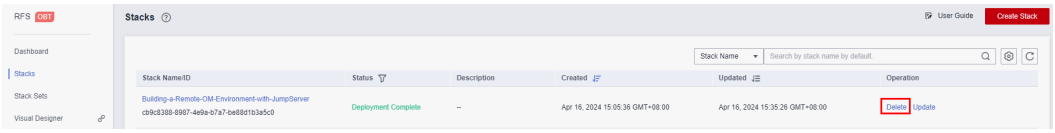


----End

3.4 Quick Uninstallation

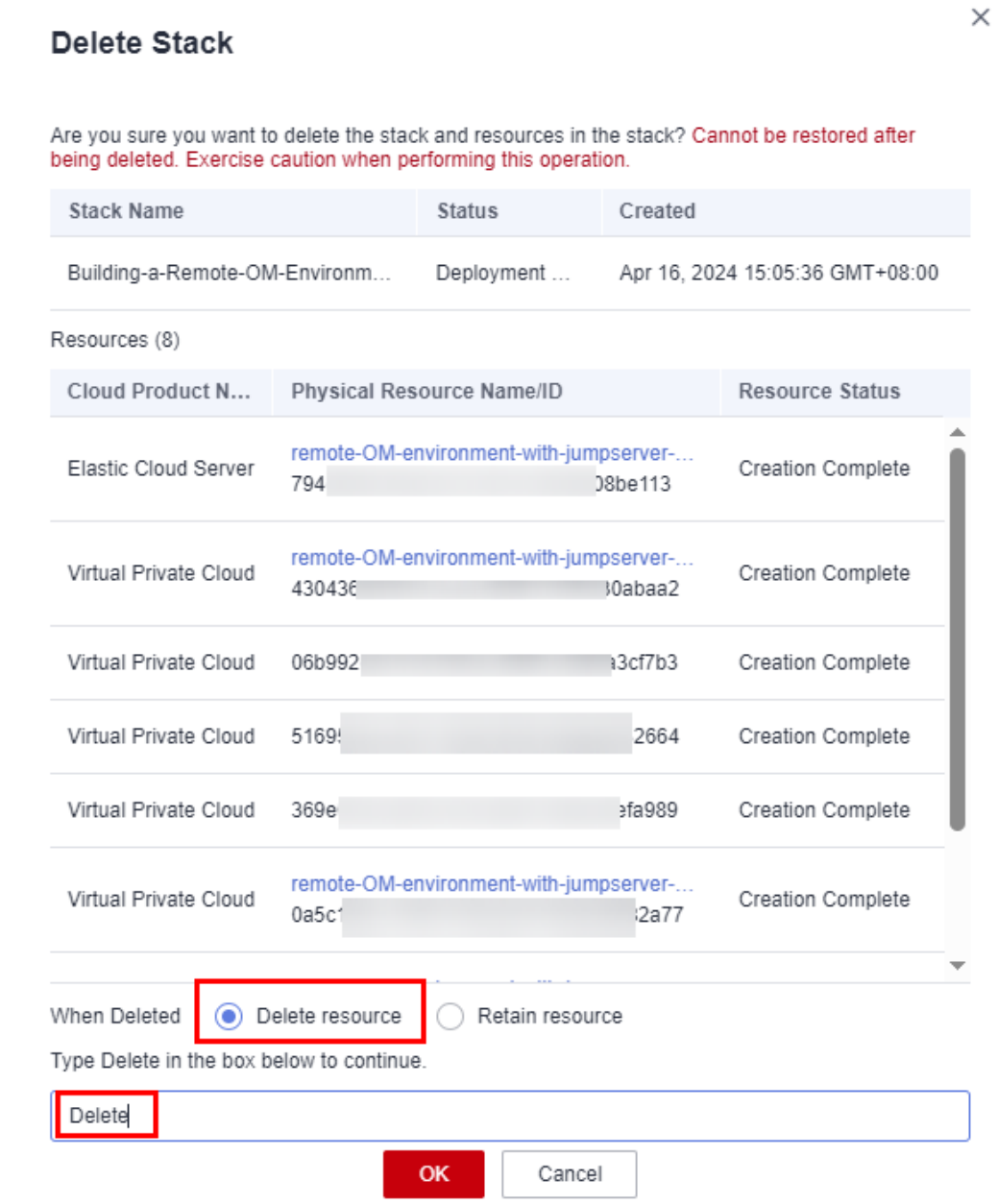
Step 1 Log in to the **RFS console**. On the **Stacks** page, locate the resource stack you created and click **Delete** in the **Operation** column.

Figure 3-22 Deleting a stack



Step 2 In the displayed **Delete Stack** dialog box, set **When Deleted** to **Delete resource**, enter "Delete" and click **OK**.

Figure 3-23 Confirming the deletion



----End

4 Appendix

Terms

Concepts, cloud service introduction, and 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 enables your cloud resources to communicate with the Internet using static public IP addresses and scalable bandwidth. EIPs can be bound to or unbound from ECSs, BMSs, virtual IP addresses, load balancers, and NAT gateways.
- Virtual Private Cloud (VPC): A VPC is an isolated and private virtual network environment. You can configure IP address segments, subnets, and security groups, as well as assign elastic IP addresses and allocate bandwidth in a VPC.
- Security group: A security group is a collection of access control rules for ECSs that have the same security protection requirements and are mutually trusted in a VPC. After you create a security group, you can create different access rules for the security group to protect the ECSs that are added to that security group.

5 Change History

Released on	Description
2024-04-16	This issue is the first official release.

