ALIBABA CLOUD

Alibaba Cloud

Bastion Host
User Guide (V3.2)

Document Version: 20220707

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Administrator manual

1.1. Authorize Bastionhost to access cloud resources

When you use Bastionhost for the first time, authorize it to access other cloud resources. This topic describes how to perform the authorization.

Prerequisites

- A bastion host is created. For more information, see Purchase a bastion host.
- An Alibaba Cloud account or a Resource Access Management (RAM) user that has permissions to create and delete service-linked roles is used.

Context

When you use Bastionhost for the first time, Alibaba Cloud automatically creates a service-linked role AliyunServiceRoleForBastionhost, which allows Bastionhost to access other cloud services. You do not need to manually create or modify the service-linked role. For more information, see Service-linked roles.

Procedure

1.
2. In the **Welcome to Bastionhost** dialog box, click **Create**.

   When you log on to the Bastionhost console for the first time after your bastion host is created, the console prompts you to authorize Bastionhost to access other cloud resources.

   After you click **Create**, Alibaba Cloud automatically creates the AliyunServiceRoleForBastionhost role. You can view the created role on the **Roles** page of the RAM console. Your bastion host can access other cloud services, such as Alibaba Cloud Elastic Compute Service (ECS) and Virtual Private Cloud (VPC), or perform server O&M and audit only after the AliyunServiceRoleForBastionhost role is created.

Service-linked role for Bastionhost

If you want to use Bastionhost for O&M, it needs to access other cloud services, such as ECS and VPC. To obtain the access permissions, you must assume the AliyunServiceRoleForBastionhost role that is automatically created for Bastionhost.

The following list provides details of the AliyunServiceRoleForBastionhost role:

- Role: AliyunServiceRoleForBastionhost
- Permission policy: AliyunServiceRolePolicyForBastionhost

  > **Note** This is a system policy. You are not allowed to modify the name or content of this policy.

- Example:

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeImages",
                "ecs:DescribeZones",
                "ecs:DescribeRegions",
                "ecs:DescribeTags",
                "ecs:DescribeSecurityGroups",
                "ecs:DescribeSecurityGroupAttribute",
                "ecs:AuthorizeSecurityGroup",
                "ecs:DescribeSecurityGroups",
                "ecs:DescribeSecurityGroupReferences",
                "ecs:CreateSecurityGroup",
                "ecs:RevokeSecurityGroup",
                "ecs:DeleteSecurityGroup",
                "ecs:ModifySecurityGroupAttribute",
                "ecs:ModifySecurityGroupPolicy",
                "ecs:ModifySecurityGroupRule",
                "ecs:CreateNetworkInterface",
                "ecs:DeleteNetworkInterface",
                "ecs:DescribeNetworkInterfaces",
                "ecs:CreateNetworkInterfacePermission",
                "ecs:DescribeNetworkInterfacePermissions",
                "ecs:DeleteNetworkInterfacePermission",
                "ecs:DetachNetworkInterface",
                "ecs:AttachNetworkInterface"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:DescribeVpcAttribute",
                "vpc:DescribeVSwitchAttributes"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ram:DeleteServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "bastionhost.aliyuncs.com"
                }
            }
        }
    ]
}
```

Delete the AliyunServiceRoleForBastionhost role

If you no longer use Bastionhost, you can delete its service-linked role AliyunServiceRoleForBastionhost. Before you can delete the AliyunServiceRoleForBastionhost role, you must release your bastion host. Then, perform the following steps:

1. Log on to the RAM console.
2. In the left-side navigation pane, click **Roles**.
3. Search for the AliyunServiceRoleForBastionhost role and click **Delete** in the Actions column.
4. In the Delete Role message, click **OK**.

FAQ

The system does not create the AliyunServiceRoleForBastionhost role for my RAM user. What do I do?

The system creates and deletes the AliyunServiceRoleForBastionhost role only if your RAM user has the required permissions. To obtain the required permissions, add the following policy to your RAM user. For more information, see Grant permissions to a RAM role.

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateServiceLinkedRole"
            ],
            "Resource": "acs:ram:*:ID of your Alibaba Cloud account:role/*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "bastionhost.aliyuncs.com"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

1.2. Log on to a bastion host

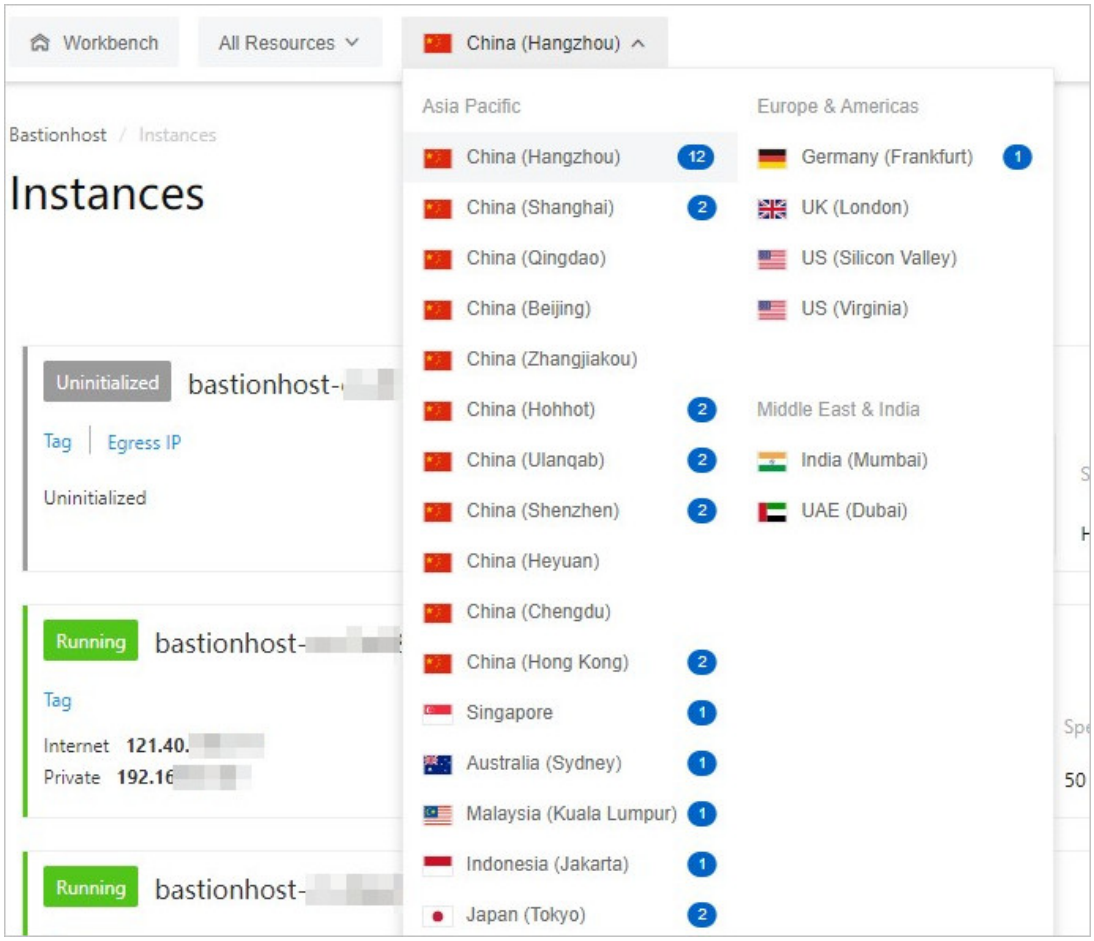
This topic describes how to log on to a bastion host from a browser.

Context

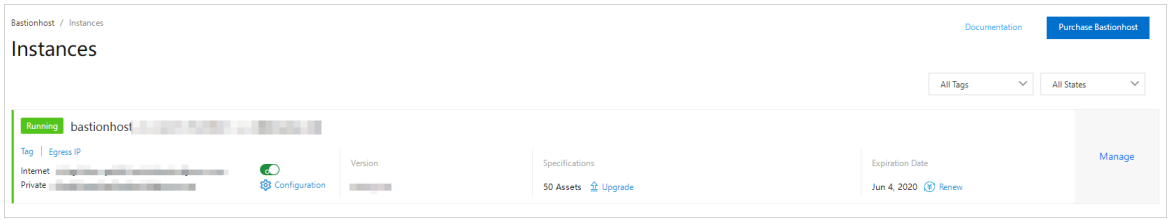
You can use an Alibaba Cloud account or a RAM user to log on to the web page of the bastion host.

Procedure

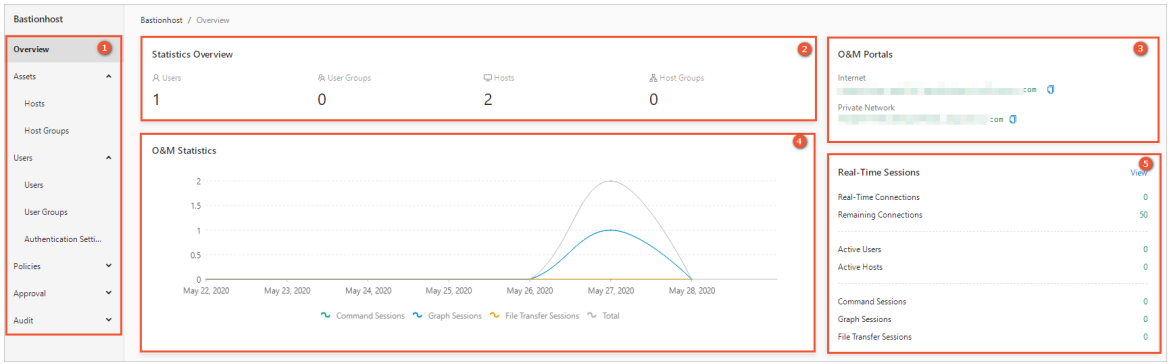
1.
2. In the top navigation bar, select a region.



3. Find the bastion host that you want to access and click **Manage**.



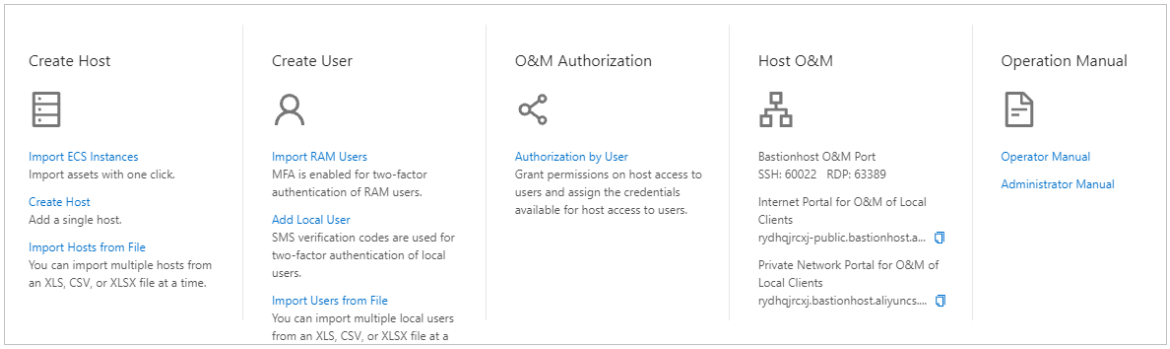
4. On the **Overview** page, view information in **Statistics Overview**, **Bastion Host Information**, **O&M Statistics**, and **Real-Time Sessions**.



The following table describes the layout of the **Overview** page.

No.	Description
1	The menu items of the bastion host.
2	The information about numbers of existing users, user groups, hosts, and host groups in the bastion host.
3	The public and internal portals of the bastion host. Users can use the portals to access the bastion host from a client and perform O&M operations.
4	The O&M statistics.
5	The information about real-time sessions.

You can click **Wizard** in the upper-right corner to perform O&M operations based on the information in the wizard. For example, you can click **Import ECS Instances** to go to the **Hosts** page and import an Elastic Compute Service (ECS) instance with a few clicks.



1.3. Instances

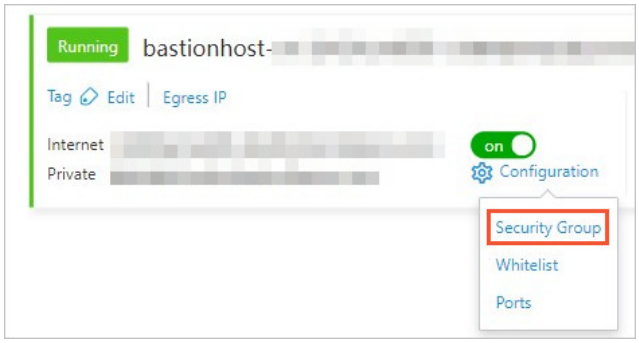
1.3.1. Configure a bastion host

After you enable a bastion host, you can configure the security group, whitelist, and port number of the bastion host in the bastion host list. This topic describes how to configure a bastion host.

Configure a security group

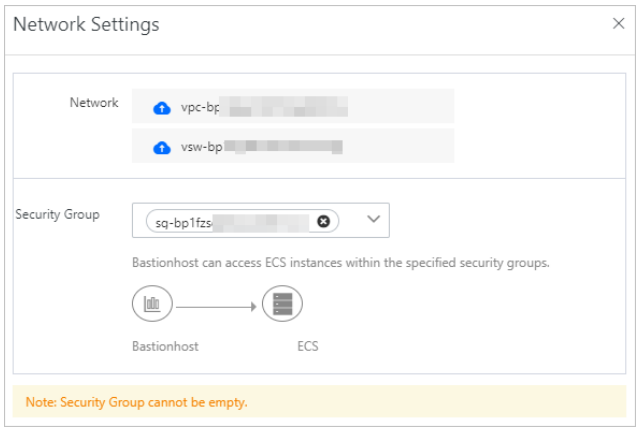
You can configure a security group to allow a bastion host to access Elastic Compute Service (ECS) instances within the security group.

1.
2. In the bastion host list, find a bastion host and click **Configuration**.
3. Select **Security Group**.



4. In the **Network Settings** panel, select the required security group.

> **Note** You can select more than one security group.

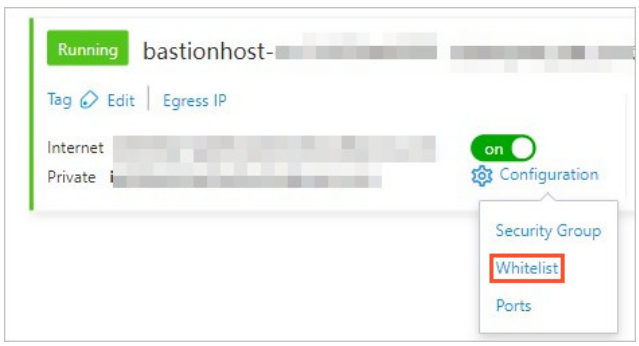


5. After the configuration is complete, click **OK**.
   After you select a security group, the bastion host can access ECS instances within the security group.

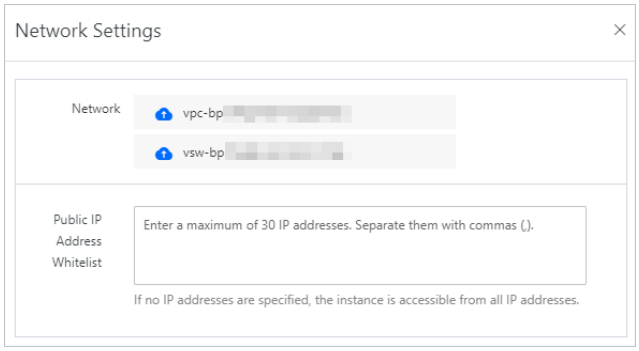
Configure a whitelist

By default, all public IP addresses can be used to log on to a bastion host for O&M. If you want to deny the logon requests from specific public IP addresses, you can add trusted IP addresses to the whitelist of the bastion host.

1.
2. In the bastion host list, find a bastion host and click **Configuration**.
3. Select **Whitelist**.



4. In the **Network Settings** panel, specify **Public IP Address Whitelist**.

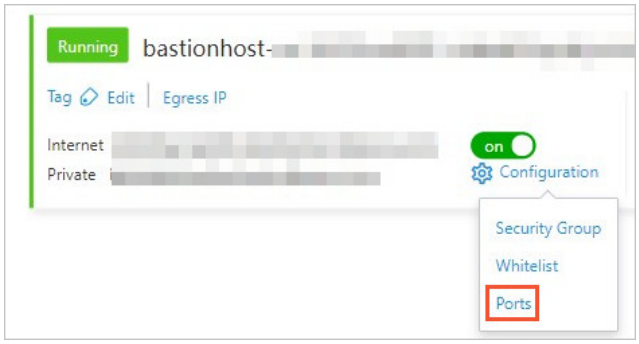


5. After the configuration is complete, click **OK**.
   The public IP addresses that can be used to log on to the bastion host are added to the whitelist.

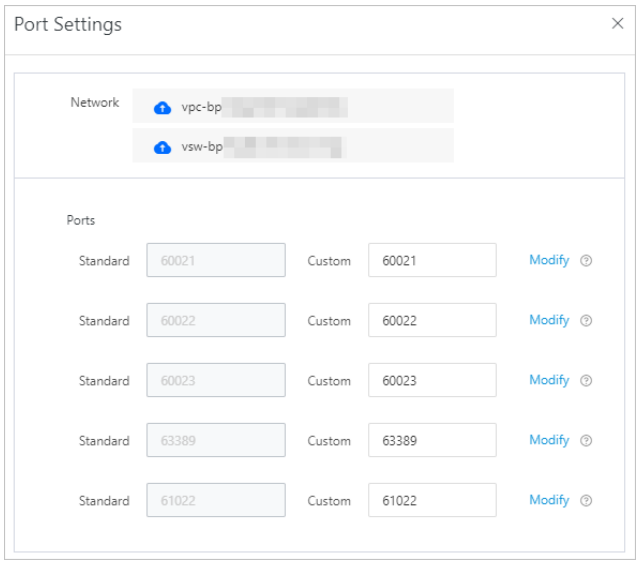
Configure a port number

If you want to change the O&M port of a bastion host, you can configure a port number for the bastion host.

1.
2. In the bastion host list, find a bastion host and click **Configuration**.
3. Select **Ports**.



4. In the **Port Settings** panel, specify **Ports**.



> **Note** The port numbers that range from 1 to 1024 are reserved for Bastionhost. We recommend that you do not specify a port number in this range.

5. After the configuration is complete, click **OK**.
   The O&M port of the bastion host is configured.

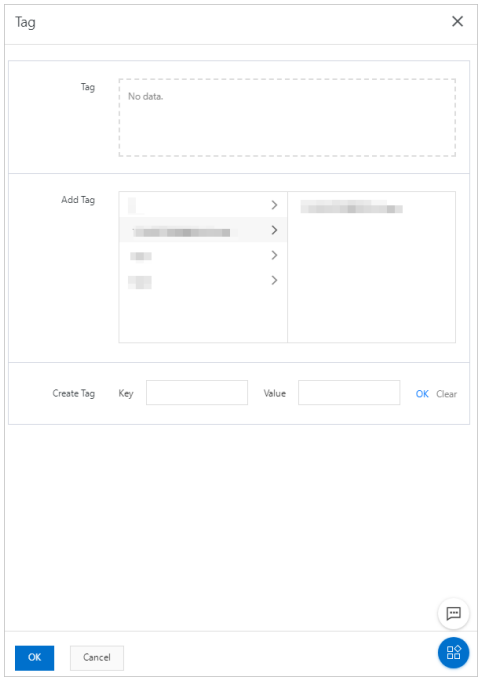
1.3.2. Manage tags of Bastionhost instances

You can add tags to Bastionhost instances to facilitate instance management. This topic describes how to add or delete tags and search for instances by tag.

Add or delete tags

1.
2. On the **Instances** page, find the target instance, move the pointer over **Tag**, and click **Edit**.

3. In the **Tag** pane, add or delete tags to or from the instance.



- **Add tags**

  You can add an existing tag or create a new tag for the instance.

  > **Note** Each tag consists of a tag key and one or more tag values.

  - **Add an existing tag**

    In the Add Tag section, select a tag key and its value.

- **Create a tag**

  In the **Create Tag** section, specify **Key** and **Value** and click **OK**.

- **Delete tags**

  If you no longer need to use a tag, click the icon that follows the tag in the Tag section to delete it.

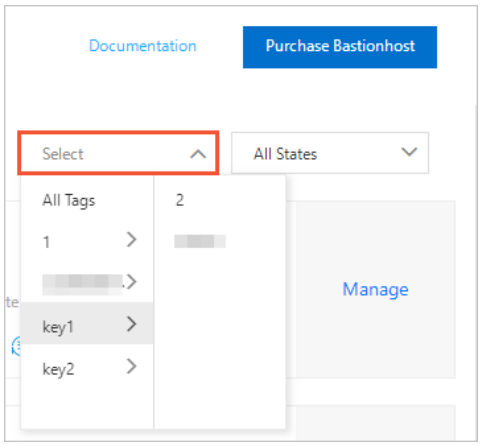
  

All tags for the instance are displayed in the **Tag** section.

4. Click **OK**.

Search for instances by tag

On the **Instances** page, select a tag key and a tag value from the drop-down list in the upper-right corner. The information of the matching instance is displayed.



1.4. Asset management

1.4.1. Host management

1.4.1.1. Add hosts

This topic describes how to import hosts to a bastion host. You can import Alibaba Cloud Elastic Compute Service (ECS) instances to a bastion host. You can also import hosts from other sources to a bastion host. After you import or add hosts to a bastion host, the O&M personnel can use the bastion host to manage the hosts.

Import ECS instances

You can perform the following steps to import ECS instances that belong to your Alibaba Cloud account to a bastion host at a time. Before you import ECS instances to a bastion host, make sure that you created ECS instances. For more information, see Connection methods.

> **Note** This operation does not affect the current status of the imported ECS instances.

1.
2.
3.
4. In the **Select Region** dialog box, select the region where the ECS instances you want to import reside and click **OK**.
5. In the **Import ECS Instances** dialog box, select the ECS instances that you want to import and click **Import**.

Import hosts from other sources

You can manually specify host information to import a host on which you want to perform O&M operations to a bastion host.

1.
2.
3. Select **Create Host** from the **Import Other Hosts** drop-down list.
4. In the Create Host panel, configure the Operation System, Host IP Address, and Hostname parameters. Then, click **Create**.

Import hosts from an ApsaraDB MyBase dedicated cluster

You can import hosts from a dedicated cluster to a bastion host at a time.

> **Note**
> - Dedicated Host Group is renamed ApsaraDB MyBase.
> - For more information about how to access a host in a dedicated cluster, see Log on to a host by using a bastion host in Linux.

1.
2.
3. Select **Import Host From Dedicated Cluster** from the **Import Other Hosts** drop-down list.
4. In the **Import Host From Dedicated Cluster** dialog box, select the hosts that you want to import and click **Import**.

Import hosts by using a template file

The template package that you download contains template files in the *XLS*, *CSV*, and *XLSX* formats. You can use one of the template files to import hosts to a bastion host at a time.

1.
2.
3. Select **Import Hosts from File** from the **Import Other Hosts** drop-down list.
4. In the **Import Hosts** panel, click **Download Host Template** to download the template package. Decompress the packet, open a template file, and then enter information about the hosts that you want to import based on the requirements of the template file. Then, save the changes to the file.

5. In the **Import Hosts** panel, click **Upload** to upload the template file that you saved.
6. In the **Preview** dialog box, select the hosts that you want to import and click **Import**.
7. In the **Import Hosts** panel, confirm the host information and click **Import Hosts**.

Import a host from a third-party asset source

You can import a host from a third-party asset source by using the access credentials and the API that is provided by the third-party asset source. Before you import a host from a third-party asset source to a bastion host, make sure that you added the third-party asset source to the bastion host. For more information, see Manage third-party asset sources.

1.
2.
3. In the Import Other Hosts drop-down list, select the name of the third-party asset source whose host you want to import.
4. In the **Import Third-party Hosts** dialog box, select the host that you want to import and click **Import**.

Related operations

- After you import hosts to a bastion host, you must create accounts for the hosts. For more information, see Create an account for a host.
- If you do not use the default port for the RDP or SSH protocol on a host, you must change the default port to the port that is used by the host in a bastion host. For more information, see Change the service port of a host.

1.4.1.2. Manage a host

This topic describes how to search for a host, modify the basic information about a host, and delete a host from the host list.

Prerequisites

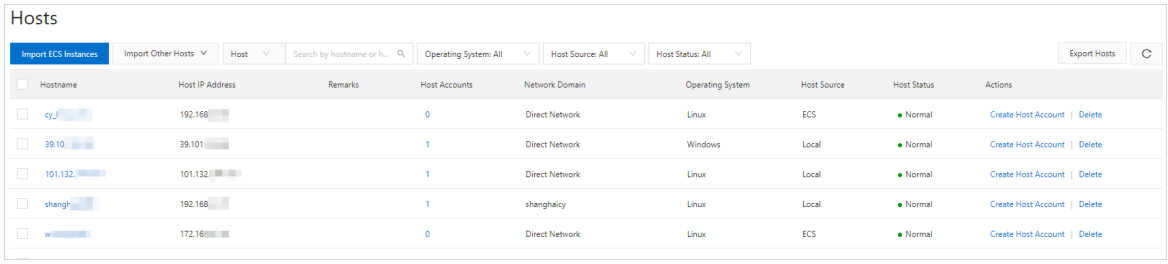
The host that you want to maintain is created in your bastion host. For more information, see Add hosts.

Limits

You can modify the basic information about hosts that are manually created or imported by using a file. You cannot modify the basic information about imported Elastic Compute Service (ECS) instances or ApsaraDB MyBase dedicated clusters.

Search for a host

1.
2.
3. On the **Hosts** page, configure filter conditions to search for a host.



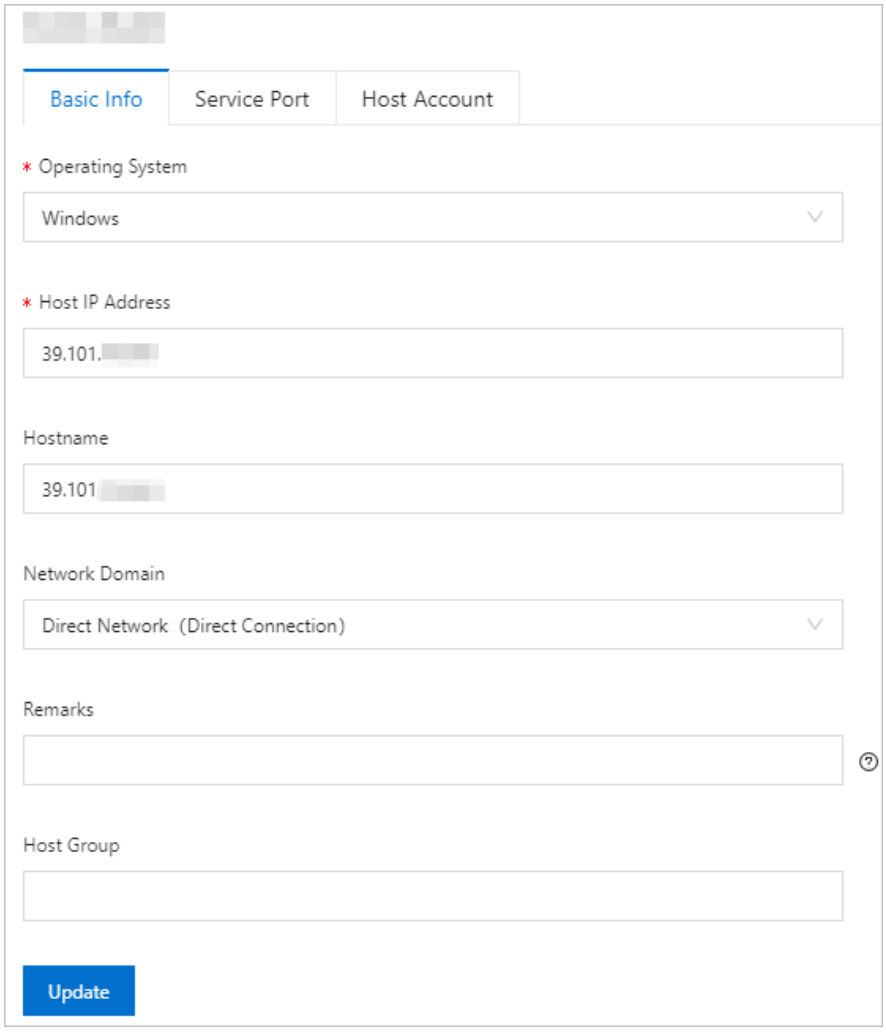
You can search for a host by using the following filter conditions:

- **Search by hostname or host IP address**: Enter the name or IP address of a host. Then, click the icon to search for the host. Fuzzy search is supported.
- **Search by operating system**: Select an operating system type. You can select **Operating System: All**, **Linux**, or **Windows**.
- **Search by host source**: Select a host source. You can select **Host Source: All**, **Local**, **ECS**, or **ApsaraDB Dedicated Cluster**.
- **Search by host status**: Select a host state. You can select **Host Status: All**, **Normal**, or **Released**. You can use Bastionhost to check whether ECS instances and ApsaraDB MyBase dedicated clusters are released. If an ECS instance or an ApsaraDB MyBase dedicated cluster is released, Bastionhost sets the **Host Status** parameter of the host to **Released**. If an ECS host or an ApsaraDB MyBase dedicated cluster is not released, Bastionhost sets the **Host Status** parameter of the host to **Normal**. You can select **Released** as a filter condition to search for all released hosts. This way, you can delete the released hosts in a convenient manner.

> **Note** If you configure multiple filter conditions at the same time, Bastionhost displays the hosts that meet all filter conditions.

Modify the basic information about a host

1.
2.
3. On the **Hosts** page, find the host whose basic information you want to modify and click the name of the host.
4. Modify the **Operating System**, **Host IP Address**, **Hostname**, **Network Domain**, **Remarks**, and **Host Group** parameters of the host.



Note You cannot modify the Host IP Address or Hostname parameters of an ECS instance.

5. Click **Update**.
   After you modify the basic information about the host, the new settings immediately take effect.

Delete a host

If you no longer need to maintain a host, you can delete the host from the host list.

1.
2.
3. On the **Hosts** page, delete a host.
   - **Delete a host**: Find the host that you want to delete and click **Delete** in the **Actions** column. You can also select the host and click **Delete** in the lower part of the host list.
   - **Delete multiple hosts**: Select the hosts that you want to delete and click **Delete** in the lower part of the host list.
4. In the **Are you sure you want to delete the selected hosts?** message, click **Delete**.
   After you delete the host, all permissions on the host are deleted. For example, if a user is granted the permissions to manage the host, the permissions are revoked when the host is deleted. You can no longer log on to the host by using Bastionhost.

1.4.1.3. Change the service port of a host

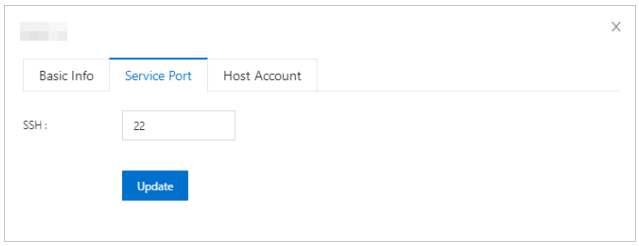
Bastionhost uses default ports for the RDP and SSH protocols (port 3389 for RDP and port 22 for SSH) as service ports of hosts. If you have customized a protocol port on a host, you must also change the matching service port in Bastionhost. This topic describes how to change the service port of a host in Bastionhost.

Prerequisites

Before you change the service port, make sure that the service port you want to use is the same as the protocol port on the host. Otherwise, you cannot log on to the host in Bastionhost.

Change the service port of a single host

1.
2.
3. On the **Hosts** page, find the target host and click the hostname.
4. In the pane that appears, click the **Service Port** tab.
5. Change the port for **RDP** or **SSH** as required.

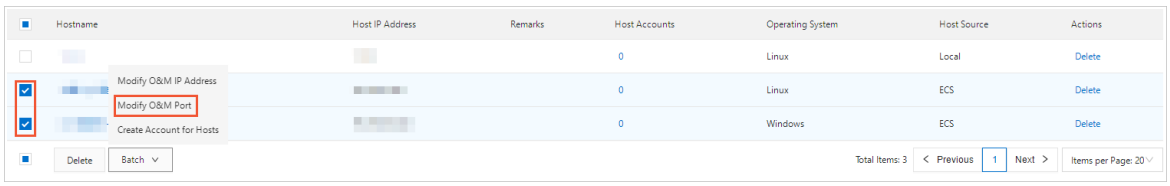


6. Click **Update**.

Change the service port of multiple hosts

If the same port is used for the same protocol of multiple hosts, follow these steps to change the port for the matching hosts at a time:

1.
2.
3. On the **Hosts** page, select the hosts whose service port you want to change and select **Modify O&M Port** from the **Batch** drop-down list in the lower-left corner.



4. In the **Modify O&M Port** dialog box, specify **Protocol** and **Port**.

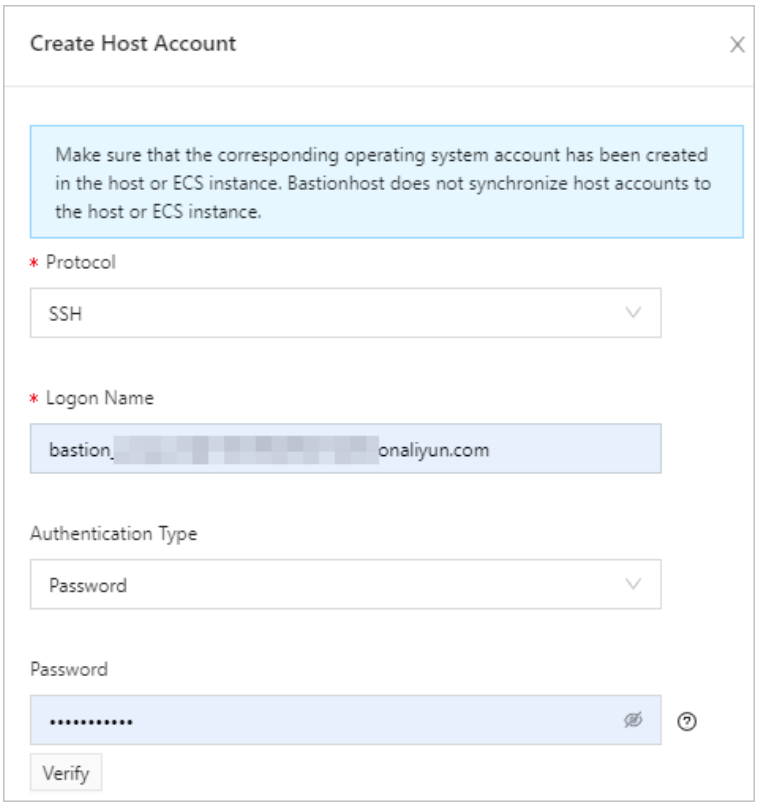
5. Click **OK**.

1.4.1.4. Create an account for a host

After you create a host, you must create and configure an account for the host in Bastionhost. This way, O&M personnel can log on to the host by using Bastionhost and perform O&M. This topic describes how to create an account for a host in Bastionhost.

Procedure

1.
2.
3. On the **Hosts** page, create an account for a host.
   - **Create an account for a host**
     a. Find the host for which you want to create an account and click **Create Host Account** in the **Actions** column.
     b. In the **Create Host Account** panel, configure the parameters such as **Protocol**, **Logon Name**, and **Authentication Type**.



c. Click **Verify**.

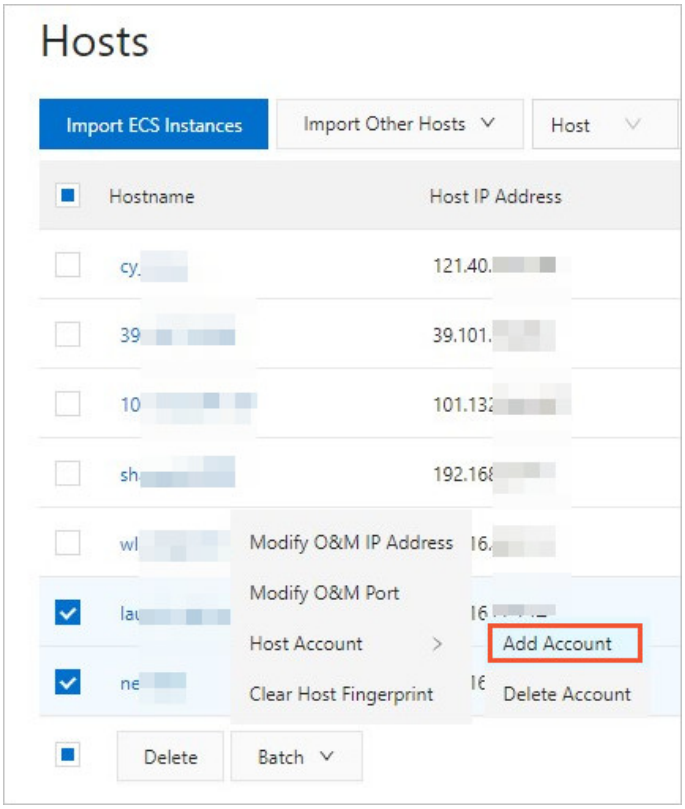
You can click **Verify** to check whether the username and password that you specify for the account are valid.

d. Click **Create**.

- **Create accounts for multiple hosts**

a. Select the hosts for which you want to create accounts.

b. In the lower part of the page, choose **Batch > Host Account > Add Account**.



c. In the Add Account dialog box, configure the parameters such as **Authentication Type**, **Protocol**, and **Logon Name**.

> **Note** When you create accounts for multiple hosts at a time, you do not need to verify the password.

d. Click **OK**.

1.4.1.5. Configure account information for a host

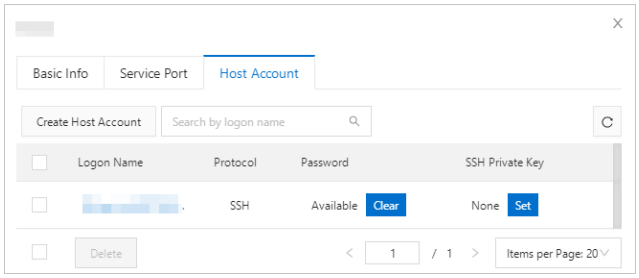
After you have created an account for a host in Bastionhost, you can modify the information of the account, delete the account, and set a password or private key for the account. This topic describes how to configure account information for a host.

Modify the information of an account

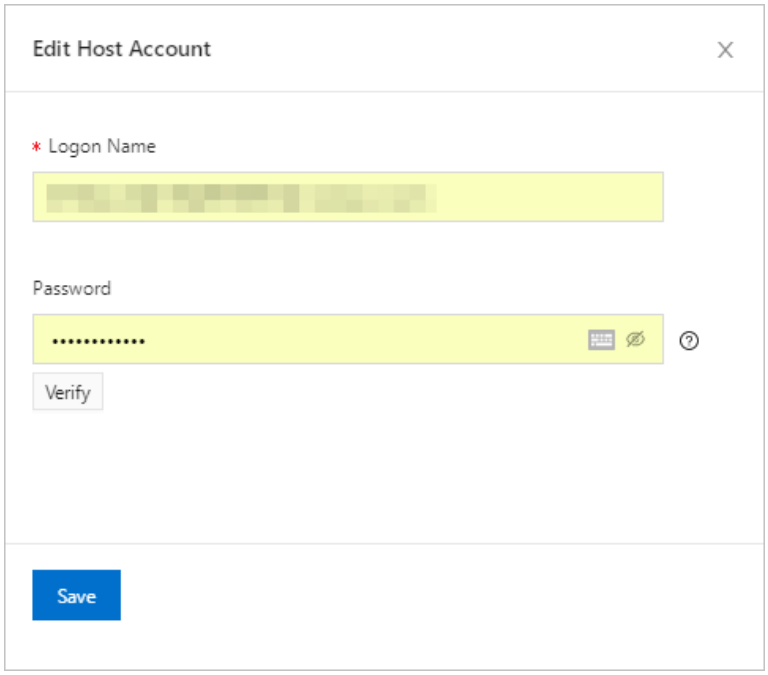
1.

2.

3. On the **Hosts** page, find the target host and click the hostname.
4. In the pane that appears, click the **Host Account** tab.



5. Find the account whose information you want to modify and click the logon name.
6. In the **Edit Host Account** pane, change the values of **Logon Name** and **Password**.

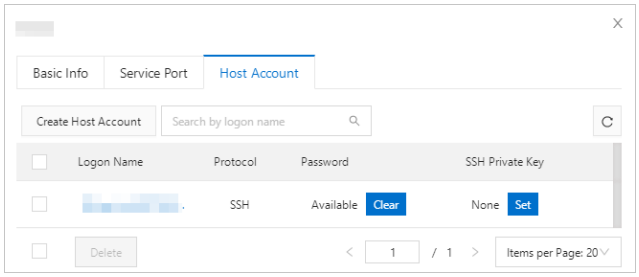


7.
8. Click **Save**.

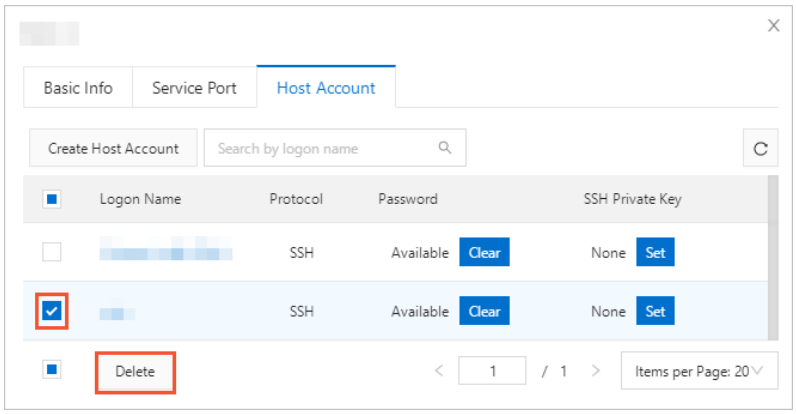
Delete an account

If you no longer need to use an account for a host, follow these steps to delete the account:

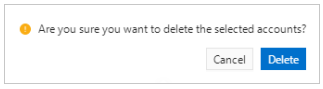
1.
2.
3. On the **Hosts** page, find the target host and click the hostname.
4. In the pane that appears, click the **Host Account** tab.



5. Select the account that you want to delete and click **Delete** in the lower-left corner.



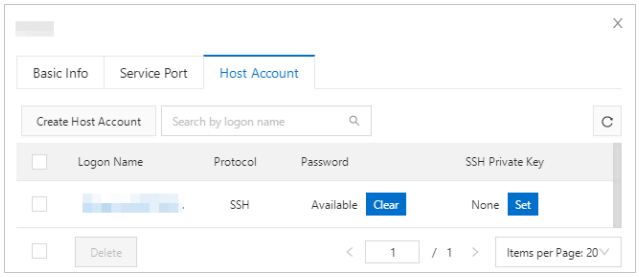
6. In the message that appears, click **Delete**.



Set a password for an account

Follow these steps to set, change, or delete a password for an account:

1.
2.
3. On the **Hosts** page, find the target host and click the hostname.
4. In the pane that appears, click the **Host Account** tab.



5. On the **Host Account** tab, set, change, or delete a password.
   - **Set or change a password**

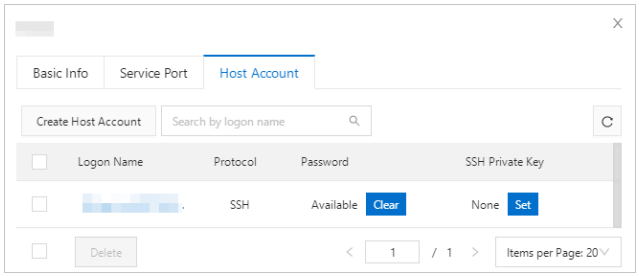
     Find the target account and click the logon name. In the **Edit Host Account** pane, enter a password.
   - **Delete a password**

     Find the target account and click **Clear** in the **Password** column.

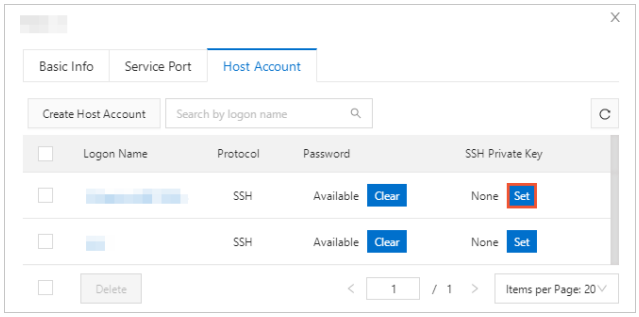
Set a private key for an account

If you want to log on to a host by using a private key in SSH mode, first set a private key for the host.

1.
2.
3. On the **Hosts** page, find the target host and click the hostname.
4. In the pane that appears, click the **Host Account** tab.

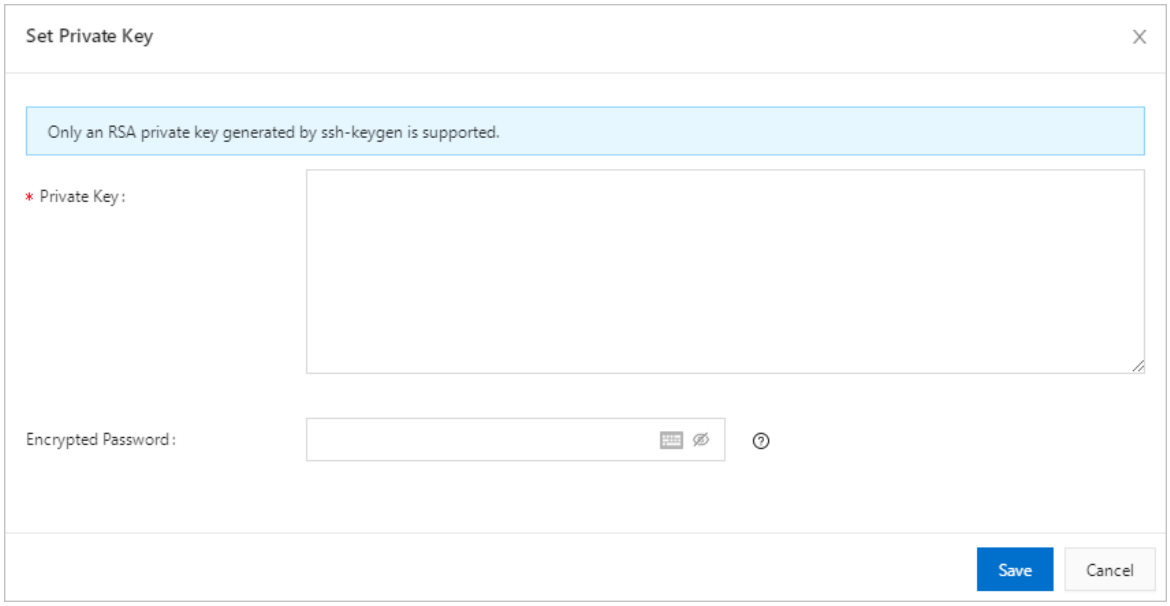


5. Find the target account and click **Set** in the **SSH Private Key** column.



6. In the **Set Private Key** dialog box, enter the private key.

> **Note**
>
> - Bastionhost supports only Rivest-Shamir-Adleman (RSA) private keys generated by **ssh-keygen**.
>
> For example, you can use the **ssh-keygen** command to generate a public key and a private key for a host that runs Linux. The public key is stored in the directory for the host, and the private key is exported to a local device. In this step, enter the generated private key.
>
> - If no encrypted password is used when the key pair is deployed on the host, leave the **Encrypted Password** field empty.



7. Click **Save**.
8. (Optional) If you want to delete the private key, click **Clear** in the **SSH Private Key** column.

1.4.1.6. Change the O&M IP address of a host

You can set either the public IP address or private IP address of a host as its O&M IP address in Bastionhost. Bastionhost connects to a host based on your settings. This topic describes how to change the O&M IP address of a host.

Context

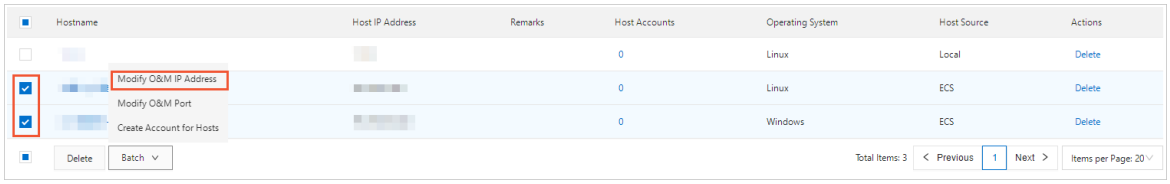
You can set the O&M IP address of a host to **Public IP Address** or **Private IP Address**:

- **Public IP Address**: Bastionhost connects to the host by using its public IP address.
- **Private IP Address**: Bastionhost connects to the host by using its private IP address.

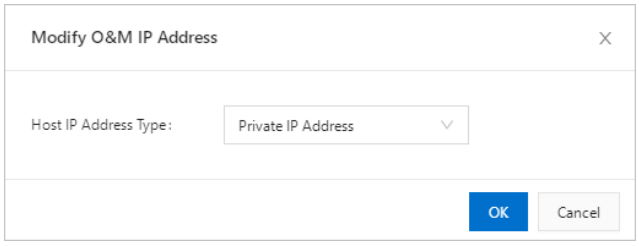
> **Note** If a host has both private and public IP addresses, Bastionhost uses the private IP address as the O&M IP address by default.

Procedure

1.
2.
3. On the **Hosts** page, select the host whose O&M IP address you want to change, and select **Modify O&M IP Address** from the **Batch** drop-down list in the lower-left corner.



4. In the **Modify O&M IP Address** dialog box, specify **Host IP Address Type**.



- If you select **Public IP Address**, Bastionhost connects to the host by using its public IP address.
- If you select **Private IP Address**, Bastionhost connects to the host by using its private IP address.

5. Click **OK**.

1.4.1.7. Clear host fingerprints

A host fingerprint is a unique identifier for Bastionhost to identify a Linux host that uses SSH. Bastionhost checks the access permissions on hosts based on host fingerprints. This prevents malicious users from accessing unauthorized hosts by using traffic redirection. If the original fingerprints of hosts are invalid, you must clear the host fingerprints. Otherwise, you cannot perform O&M operations on the hosts. This topic describes how to clear host fingerprints.

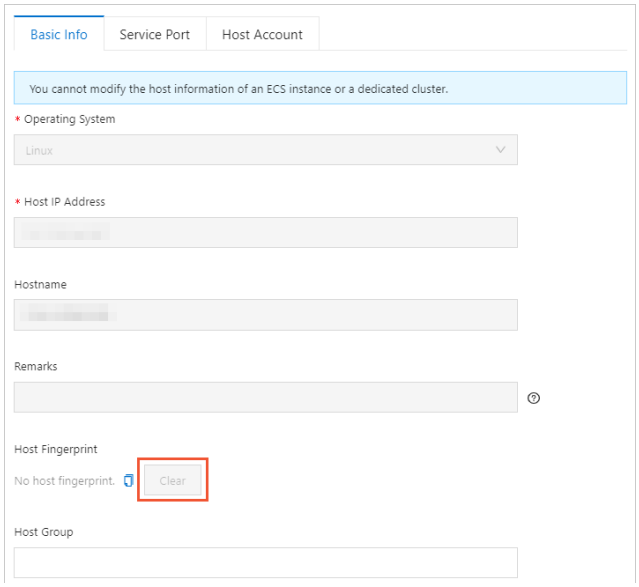
Context

Bastionhost uses a host fingerprint to uniquely identify a Linux host. If you clear the fingerprint of a host, no impacts are imposed on your O&M operations. The next time you maintain the host, Bastionhost automatically generates a new fingerprint for the host.

Clear the fingerprint of a single host

To clear the fingerprint of a single host, perform the following steps.

1. Log on to the Bastionhost console.
2.
3. Find the host whose fingerprint you want to clear and click its name.
4. On the **Basic Info** tab of the panel that appears, click **Clear** next to the host fingerprint.

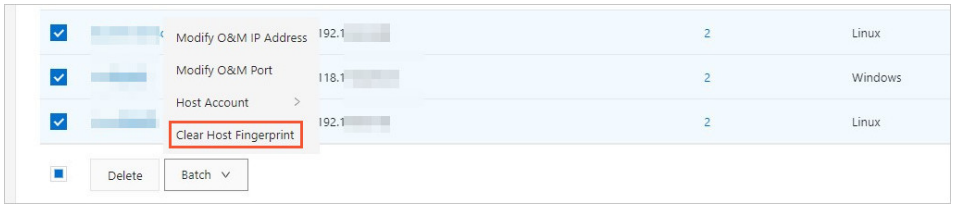


After the fingerprint is cleared, a message indicating that the host fingerprint is reset appears, and **No host fingerprint.** is displayed in the **Host Fingerprint** section of the Basic Info tab.

Clear the fingerprints of multiple hosts at a time

To clear the fingerprints of multiple hosts at a time, perform the following steps.

1.
2.
3. On the **Hosts** page, select the hosts whose fingerprints you want to clear and choose **Batch > Clear Host Fingerprint**.



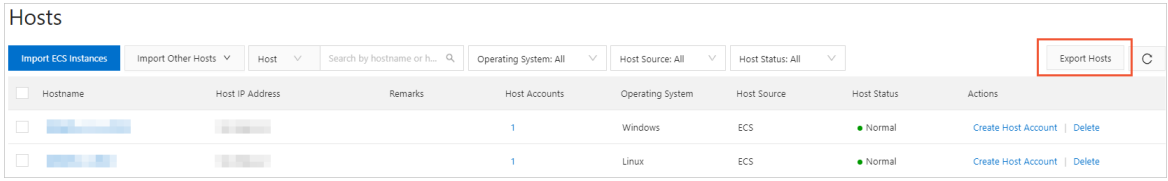
4. In the message that appears, click **OK**.
After the operation is complete, a message indicating that the host fingerprints are reset appears.

1.4.1.8. Export the host list with a few clicks

Bastionhost allows you to export the host list with a few clicks. This way, you can view the host list in a local CSV file. This topic describes how to export the host list with a few clicks.

Procedure

1.
2.
3. On the **Hosts** page, click **Export Hosts** in the upper-right corner of the host list.
The host list is exported to a CSV file.



1.4.2. Manage asset groups

You can create different asset groups based on your business requirements. Then, you can add the same type of hosts to a host group. This way, you can manage hosts of the same type at a time.

Create an asset group

1.
2.
3.
4. In the **Create Asset Group** panel, configure the Asset Group Name and Description parameters, and click **Create**.

The name of the asset group must be 1 to 128 characters in length and can contain letters, digits, periods (.), underscores (_), hyphens (-), backslashes (\), and spaces. The name cannot start with a special character.

> **Note** We recommend that you specify a descriptive asset group name to facilitate subsequent management and maintenance. For example, specify a name based on information such as the service provided by the hosts, the department to which the hosts belong, or the region where the hosts reside.

Add hosts to a host group

After you create an asset group, you can add hosts to the asset group to manage the hosts at a time Before you add hosts to an asset group, make sure that you imported or created hosts in Bastionhost. For more information, see Add hosts.

1.
2.
3. In the asset group list, click the name of the asset group to which you want to add hosts.
4. In the panel that appears, click the **Hosts** tab and then click **Add Hosts**.
5. In the **Add Member** dialog box, select the hosts that you want to add to the asset group and click **Add**.

> **Note** To add a single host, click **Add** in the **Actions** column of the host. In the message that appears, click Add.

Related operations

- Remove a host from an asset group

  On the **Asset Group** page, click the name of the asset group from which you want to remove a host. On the **Hosts** tab, select the host that you want to remove and click **Remove**. In the message that appears, click **Remove**.

- Modify the information about an asset group

  On the **Asset Group** page, click the name of the asset group whose information you want to modify. On the **Asset Group Settings** tab, modify the values of the Asset Group Name and Description parameters and click **Update**.

- Delete an asset group

  On the **Asset Group** page, find the asset group that you want to delete and click **Delete** in the **Actions** column. In the message that appears, click **Delete**.

1.4.3. Use the automatic password change feature

Bastionhost provides the automatic password change feature. The feature can randomly generate a password based on the password policy that you configure and automatically rotate the passwords of managed host accounts. This topic describes the operations related to password changes. The operations include creating and running a password change task.

Context

Multi-Level Protection Scheme (MLPS) requires that logon credentials, such as passwords, of host accounts be changed on a regular basis. If the passwords are not changed for a long period of time, security risks may arise. However, regular and manual password rotation is inefficient and is prone to errors. To resolve this issue, Bastionhost provides the automatic password change feature.

Limits

- The automatic password change feature is available only in Bastionhost HA Edition.
- Bastionhost allows you to change the passwords of accounts only for Linux hosts. You cannot change the passwords of accounts for Windows hosts.
- A password change task supports only the host accounts for which Protocol is set to SSH and Authentication Type is set to Password.

Supported OSs and versions

OS	Version
Alibaba Cloud Linux	• 3.2104 64-bit • 2.1903 LTS 64-bit • 2.1903 64-bit (Quick Start)
CentOS	All versions
Ubuntu	All versions
Debian	All versions
Open SUSE	• 15.1 64-bit • 15.2 64-bit • 42.3 64-bit **Note** You can use the automatic password change feature to change the passwords only of standard accounts. You cannot use this feature to change the passwords of root accounts.
SUSE Linux	• SUSE Linux Enterprise Server 15 SP2 64-bit • SUSE Linux Enterprise Server 12 SP5 64-bit • SUSE Linux Enterprise Server 11 SP4 64-bit
CoreOS	• 2303.4.0 64-bit • 2247.6.0 64-bit • 2023.4.0 64-bit • 1745.7.0 64-bit

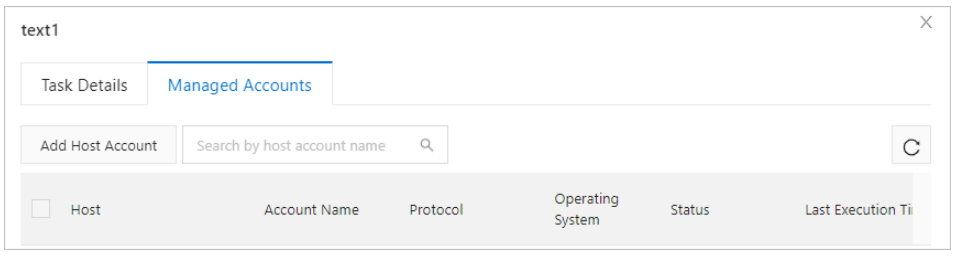
Create a password change task

1.

2.
3.
4. In the **Create Password Change Task** panel, configure the following parameters.

Parameter	Description
Task Name	The name of the password change task.
Execution Method	The execution method of the password change task. Valid values: ○ **Periodic**: If you select this option, you must also configure Executed At and Period. You must set Executed At to a point in time that is at least 5 minutes later than the current time. The maximum value of Period is 365. Executed At and Period specify a cycle. Bastionhost runs the password change task multiple times based on the values that you specify for Executed At and Period. ○ **Scheduled**: If you select this option, you must also set Executed At to a point in time that is at least 5 minutes later than the current time. Bastionhost automatically runs the password change task at the point in time that you specify.
Password Rules	The complexity and length settings of the new password. ○ **Password Strength**: the complexity settings of the new password. You can select Digits, Lowercase Letters, Uppercase Letters, and Other Characters. Bastionhost randomly generates a new password based on the character types that you select. We recommend that you select at least two character types. ○ **Password Length**: the minimum length of the new password. For example, if you set this parameter to 8, Bastionhost randomly generates a new password that is of 8 to 32 characters in length.
Remarks	The remarks of the password change task.

5. Click **Create**.
   The created task is displayed on the Password Change page.
6. Click **Associate Account**.
7. On the **Managed Accounts** tab, click **Add Host Account**.
8. In the **Add Host Account** dialog box, select the host account that you want to add and click **Add**.



Take note of the following limits when you add host accounts to password change tasks:

- A host account can be added only to one password change task.
- The Protocol parameter of a host account must be set to SSH, and a password must be specified for the account. If an SSH key or a share key is used to authenticate a host account, you cannot

add the account to the password change task.

After the operation is complete, a message appears, which indicates that **the password change task is associated with the host account**. You can view the created task on the **Password Change** page.

Immediately run a password change task

After you create a password change task, Bastionhost automatically runs the task based on the time or cycle that you specify. If you want to immediately run the task, select the task and click **Execute Now** on the **Password Change** page.

> **Note**
>
> - If you select more than one password change task, Bastionhost runs the tasks one by one.
> - If the time when you immediately run a periodic or scheduled password change task overlaps with the execution time that you specify for the task, Bastionhost runs the password change task only once. If the time when you immediately run a periodic or scheduled password change task does not overlap with the execution time that you specify for the task, the execution time or cycle that you specify for the password change task is not affected. In this case, although the password is changed after you immediately run the task, the task is still run to change the password based on the specified execution time or cycle.

Modify, enable, stop, or delete a password change task

After you create a password change task, you can modify, enable, stop, or delete the task on the **Password Change** page.

- **Modify a password change task**

  Bastionhost allows you to modify the basic information and associated accounts of a password change task. On the **Password Change** page, click the name of the task whose information you want to modify. On the **Task Details** tab of the panel that appears, modify the basic information about the task and click **Update**. To modify a managed account, click the **Managed Accounts** tab. On the **Managed Accounts** tab, add or remove host accounts.

- **Stop a password change task**

  If you no longer need one or more password change tasks within a specific period of time, you can stop the tasks. On the **Password Change** page, select the task that you want to stop and click **Stop**. After the task is stopped, the status of the task changes to **Canceled**. In this case, the task is not automatically run, and you cannot immediately run the task.

- **Enable a password change task**

  If you want to run one or more password change tasks that have been stopped, you can enable the tasks. On the **Password Change** page, select the task that you want to enable and click **Enable**. After the task is enabled, the status of the task changes to **Pending Execution**. In this case, the task is automatically run based on the execution time or cycle that you specify.

- **Delete a password change task**

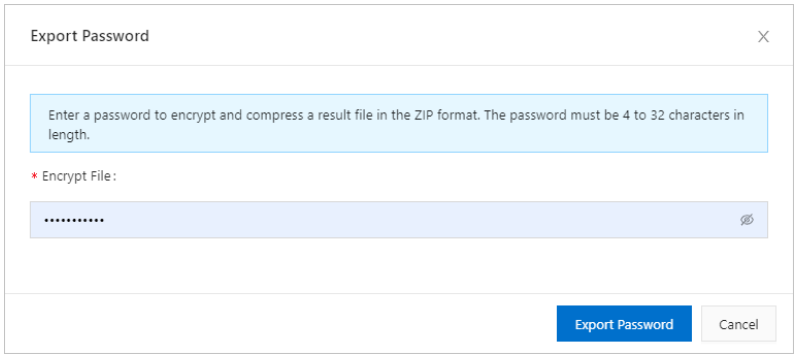
  If you no longer need one or more password change tasks, you can delete the tasks. On the **Password Change** page, select the task that you want to delete and click **Delete**. In the message that appears, click **Delete**.

> **Note** You cannot recover a password change task after you delete it. Proceed with caution.

Export a password

After a password change task is successfully run, you can use the password export feature to obtain the current password of a host account. On the **Change Password** page, find the task for which you want to export the password and click **Export Password** in the Actions column. In the **Export Password** dialog box, enter a password that is used to encrypt the exported file and click **Export Password**. The file encryption password that you entered must be 4 to 32 characters in length. The current password of the host account is exported to a *ZIP* file and saved to your computer.

> **Note** You must properly save the file encryption password that you entered in the **Export Password** dialog box. The file encryption password is required to decompress the exported file and obtain the current password of the host account.



1.4.4. Use the key management feature

Bastionhost provides the key management feature. This feature allows you to create keys and associate the keys with multiple host accounts at a time. This way, you can manage host accounts in a more efficient manner. You can modify the basic information about the keys. You can also associate the keys with multiple host accounts or disassociate the keys from the associated host accounts. This facilitates O&M. This topic describes how to create keys and modify the information about keys.

Context

If you want to use Bastionhost to save your private keys, you can deploy key pairs on hosts. Then, you can use the key management feature to create a shared key and associate the shared key with different host accounts.

Create a key

You can create a key and associate the key with a host account in the console of a bastion host. After you associate the key with the host account, the key becomes the shared key of the associated host. The shared key is preferentially used to log on to the host on which you want to perform O&M operations.

Step 1: Create a key

1.
2.
3.

4. In the **Create Key** panel, configure **Key Name**, **Key**, and **Encryption Password**.

   > **Note** You can enter only a Rivest-Shamir-Adleman (RSA) key that is generated by using the **ssh-keygen** tool.

5. Click **Create**.
   You can view the key that you created on the Keys page.

Step 2: Associate the key that you created with a host account

> **Note**
> - You can associate the key only with the host accounts whose Protocol is set to SSH.
> - You can associate a shared key with multiple host accounts. However, you can bind a host account to only one shared key.

1. On the **Keys** page, find the key that you created and click **Associate Host Account** in the **Actions** column.
2. In the **Associate Host Account** dialog box, select the host account with which you want to associate the key and click **Associate** in the lower-left corner. You can also click Associate in the **Actions** column of the host account and click **OK**.

Modify the information about a key

You can modify the basic information about a shared key on the Basic Information tab. You can also associate the shared key with a host account or disassociate the shared key from a host account on the Host Account tab.

1.
2.
3. In the key list, find the key whose information you want to modify and click **Edit** in the **Actions** column. In the panel that appears, perform the following operations based on your business requirements:
   - On the **Basic Information** tab, modify the **Key Name**, **Key**, and **Encryption Password** parameters. After you modify the parameters, click **Update**.

     > **Note** After the information on the Basic Information tab is updated, the **Last Modified At** column of the key in the key list displays the point in time when the information about the key was last modified.

   - On the **Host Account** tab, associate the shared key with a host account or disassociate the shared key from a host account.
     - Associate the shared key with a host account: Click **Associate Host Account**. In the **Associate Host Account** dialog box, select the host account with which you want to associate the key and click **Associate** in the lower-left corner. You can also click Associate in the **Actions** column of the host account and click **OK**.
     - Disassociate the shared key from a host account: In the **Actions** column of the host account from which you want to disassociate the key, click **Disassociate**.

1.4.5. Use the network domain feature

If you want to manage the servers that reside on different networks or the servers that cannot communicate with bastion hosts in virtual private clouds (VPCs) in a centralized manner, we recommend that you use the network domain feature of Bastionhost. You can configure a proxy server for these servers, create a network domain in the Bastionhost console, and then connect the network domain to the proxy server. This way, you can use the proxy server to maintain other servers. This topic describes how to use the network domain feature.

Context

The network domain feature provides the optimal O&M solutions for hybrid cloud scenarios. For example, you can use the feature to maintain servers across data centers, heterogeneous clouds, and VPCs. In most cases, the servers of an enterprise reside in different regions and may fail to communicate with a bastion host. To resolve this issue, you can use public IP addresses or leased lines to connect to the servers. However, public IP addresses may pose security risks while leased lines cause high network costs. In this case, we recommend that you use the proxy mode of the network domain feature to centrally maintain the servers that reside on different networks. The proxy mode is supported by Bastionhost HA Edition. The servers include those in a data center, a heterogeneous cloud, and different VPCs.

Limits

- The proxy mode of the network domain feature is available only in Bastionhost HA Edition.
- The network domain feature supports SSH, HTTP, and SOCKS5 proxies.

Create a network domain

To use your bastion host to maintain multiple servers in a network domain, you must create a network domain for the bastion host and connect the network domain to a proxy server.

1.
2. In the left-side navigation pane, choose **Assets > Network Domain**.
3. On the **Network Domain** page, click **Create Network Domain**.
4. In the **Create Network Domain** panel, specify the Network Domain, Remarks, and Connection Mode parameters.

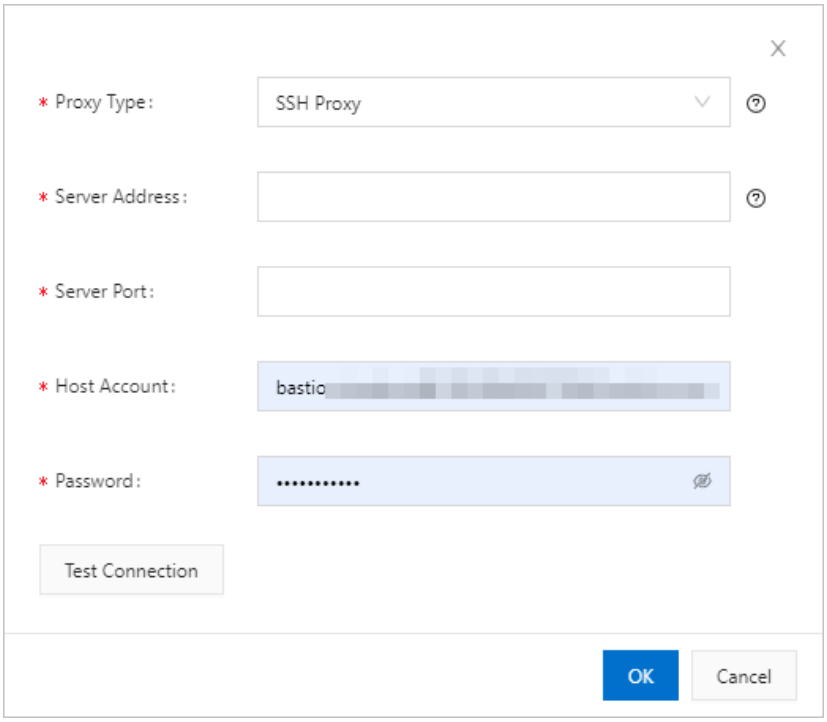
   You can select **Direct Connection** or **Proxy** for the Connection Mode parameter.

   > **Note** Bastionhost Basic Edition and HA Edition support different connection modes.
   > - Bastionhost Basic Edition supports only the direct connection mode.
   > - Bastionhost HA Edition supports the direct connection mode and the proxy mode.

   If you select **Proxy** , you must configure at least one proxy server. The network domain feature allows you to configure a primary proxy server and a secondary proxy server. You can configure a secondary proxy server in the same manner in which you configure a primary proxy server. The following example shows how to configure a primary proxy server:

   i. Click **Create Proxy Server** in the Primary Proxy Server section.

ii. In the dialog box that appears, configure the following parameters.



Parameter	Description
Proxy Type	The type of the proxy. Valid values: ■ SSH Proxy ■ HTTP Proxy ■ SOCKS5 Proxy
Server Address	The address of the primary proxy server.
Server Port	The port of the primary proxy server.
Host Account	The account of the primary proxy server.
Password	The password of the account for the primary proxy server.

iii. Optional. Repeat the proceeding steps to configure the secondary proxy server.

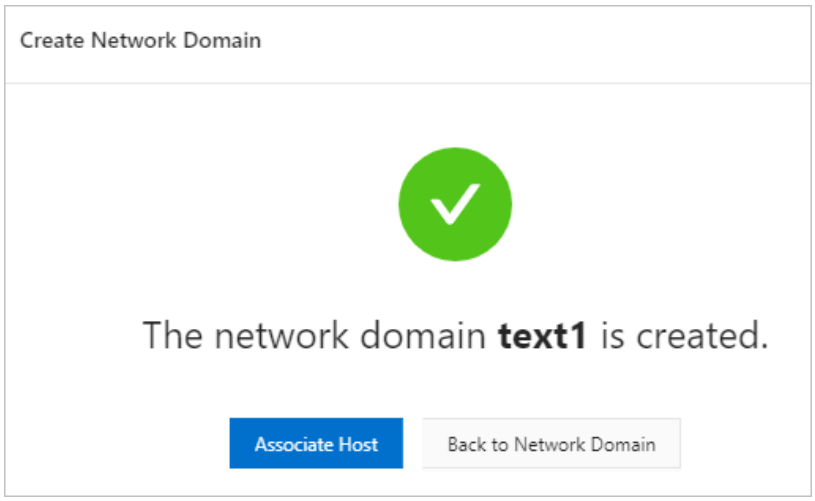
> **Note** The network domain feature supports two proxy servers: **primary proxy server** and **secondary proxy server**. If an error occurs on the primary proxy server, the secondary proxy server is automatically connected to your bastion host. To ensure the stability of the network domain, we recommend that you configure a secondary proxy server.

iv. Click **Test Connection**.

> **Note** If the connectivity test fails, check whether the parameters are correctly configured.

v. Click **OK**.

5. Click **Create Network Domain**. The system displays the message "The network domain text1 is created."
   You can click **Associate Host** below the message to add the hosts that you want to maintain to the network domain. For more information, see Add hosts.



Add hosts

After you create a network domain, you can add hosts to the network domain.

1.
2. In the left-side navigation pane, choose **Assets > Network Domain**.
3. On the **Network Domain** page, find the network domain to which you want to add hosts.
4. Click **Add Host** in the Actions column.
5. In the **Add Host** dialog box, find the host that you want to add to the network domain and click **Add Host** in the Actions column.

   You can also select multiple hosts that you want to add to the network domain and click **Add Host** below the host list to add the selected hosts at a time.

Edit a network domain

You can edit the basic information about a network domain. You can also add hosts to or remove hosts from a network domain.

1.
2. In the left-side navigation pane, choose **Assets > Network Domain**.
3. On the **Network Domain** page, find the network domain whose information you want to edit.
4. Click **Edit** in the Actions column.
5. On the Network Domain Details page, modify the information on the **Basic Info** and **Host** tabs.
   - On the **Basic Info** tab, you can change the values of **Network Domain**, **Connection Mode**, and **Remarks**. You can also **edit** and **test the connectivity** to the primary and secondary proxy servers.
   - On the **Host** tab, you can add or remove hosts.

What's next

After you connect your bastion host to the servers in a network domain by using the network domain

feature, you must authorize hosts for your bastion host to maintain the servers in the network domain.

- Authorize hosts. For more information, see Authorize a user to manage hosts and Authorize a user to manage host groups.
- Maintain servers. For more information, see Perform O&M operations on hosts.

1.5. Manage users

1.5.1. User management

1.5.1.1. Manage users

After a Bastionhost administrator adds a user for an O&M administrator, the O&M administrator can log on to the required bastion host as the user. This topic describes how to add a user, modify the user information, lock or unlock the user, host the public key of the user, and delete the user in the console of a bastion host.

User types

In the console of a bastion host, you can import Alibaba Cloud Resource Access Management (RAM) users, create local users, and import Active Directory (AD)-authenticated or Lightweight Directory Access Protocol (LDAP)-authenticated users. The following table describes how to add different types of users.

User type	Scenario
RAM user	If a RAM user is created for an O&M administrator, you can click Import RAM Users to import the RAM use. Then, the O&M administrator can use the RAM user to log on to the required bastion host.
Local user	You can choose Import Other Users > Create User or Import Other Users > Import Users from File to create accounts for O&M administrators. This allows O&M administrators to log on to the required bastion host.
AD-authenticated user	You can configure AD authentication on a bastion host and import an AD-authenticated user to the bastion host. Then, an O&M administrator can use the AD-authenticated user to log on to the bastion host. Before you import the AD-authenticated user, make sure that you configured AD authentication. For more information, see Configure AD authentication.
LDAP-authenticated user	You can configure LDAP authentication on a bastion host and import an LDAP-authenticated user to the bastion host. Then, an O&M administrator can use the LDAP-authenticated user to log on to the bastion host. Before you import the LDAP-authenticated user, make sure that you configured LDAP authentication. For more information, see Configure LDAP authentication.

Add users

You can import RAM users, create local users, and import AD-authenticated or LDAP-authenticated users based on your business requirements. Then, O&M administrators can use the RAM users, accounts of the local users, AD-authenticated users, or LDAP-authenticated users to log on the required bastion hosts.

Import one or more RAM users

1.
2.
3.
4. If no RAM user is created, click **Create RAM User** in the **Import RAM Users** dialog box and create a RAM user as prompted.

   For more information, see Create a RAM user.
5. In the **Import RAM Users** dialog box, click **Import** in the **Actions** column of the RAM user that you want to import. If you want to import multiple RAM users at a time, select the RAM users that you want to import and click **Import** in the upper-left corner.

Create one or more local users

1.
2.
3. Create a single local user or import multiple local users from a file based on the steps described in the following table.

Scenario	Procedure
	i. Choose **Import Other Users > Create User**. ii. In the **Create User** panel, configure the parameters and click **Create**. You can configure the basic information about the local user, such as **Username**, **Password**, **User Group**, and **Remarks**. You can also perform the following operations: ■ Select **Users must reset the password at next logon**: If you select this parameter, the local user must reset the password upon the next logon. This parameter is valid only for local users. ■ Specify **Validity Period**: After the validity period that you specified for the local user elapses, the status of the local user in the **Status** column is changed to **Expired**. An O&M administrator cannot use the local user to log on to the bastion host.

Scenario	Procedure
Create a single local user	■ Configure **Two-factor Authentication Methods**: If you enable Two-factor Authentication Methods, the local user must enter a dynamic verification code that is sent by text message, email, or DingTalk after the local user enters the valid password. This helps reduce security risks. **Note** ■ If you enable Two-factor Authentication Methods for a local user, the local user must enter a dynamic verification code that is sent by text message or email when the local user attempts to log on to the required bastion host. Make sure that you enter the valid mobile phone number or email address of the local user. For more information about the countries and areas where SMS-based two-factor authentication is supported, see Supported countries and areas for SMS-based two-factor authentication. ■ The mobile phone number and email address that you entered are used only to receive verification codes or alert notifications. Valid values of **Two-factor Authentication Methods**: ■ **For All Users**: specifies that the global two-factor authentication methods are used. The global two-factor authentication methods are the two-factor authentication methods that you configure on the **System Settings** page. For more information, see Enable two-factor authentication. ■ **For Single User**: specifies that you must configure a separate two-factor authentication method for the local user. Bastionhost supports the following two-factor authentication methods: ■ **Disable**: specifies that two-factor authentication is disabled. ■ **Text Message**: specifies that two-factor authentication is implemented by using text messages. If you select this method, you must specify the mobile phone number of the local user. ■ **Email**: specifies that two-factor authentication is implemented by using emails. If you select this method, you must specify the email address of the local user. ■ **DingTalk**: specifies that two-factor authentication is implemented by using DingTalk notifications. If you select this method, you must specify the mobile phone number of the local user. **Note** If you select DingTalk when you enable two-factor authentication, make sure that the following requirements are met:

Scenario	Procedure
Import multiple local users from a file	i. Select **Import Users from File** from the **Import Other Users** drop-down list. ii. Click **Download User Template**, download the user template package to your computer, and decompress the package. Then, enter the information about the local users that you want to import in a user template file, and save the information. iii. In the **Import Local Users** dialog box, click **Upload** to upload the user template file that you edited. iv. In the **Preview** dialog box, select the local users that you want to import and click **Import**. v. In the **Import Local Users** panel, confirm the information about the local users. If you select **Users must reset the password at next logon**, all imported local users must reset their passwords upon the next logon. vi. Click **Import Local Users**. **Note** The local users that you want to import are displayed in a table. If some local users, for example, the first user, the third user, and the fifth user, share the same username, the bastion host imports only the fifth user. If a local user that you want to import shares the same username with an existing user in the bastion host, the information about the existing user is overwritten by the information about the local user that you want to import. You can click **Details** in the **Import Local Users** panel to view the information about the users that are not imported.

Import one or more AD-authenticated users

1.
2.
3. Choose **Import Other Users > Import AD Users**.
4. In the **Import AD Users** dialog box, click **Import** in the **Actions** column of the AD-authenticated user that you want to import. If you want to import multiple AD-authenticated users at a time, select the AD-authenticated users that you want to import and click **Import** in the upper-left corner.

Import one or more LDAP-authenticated users

1.
2.
3. Choose **Import Other Users > Import LDAP Users**.
4. In the **Import LDAP Users** dialog box, click **Import** in the **Actions** column of the LDAP-authenticated user that you want to import. If you want to import multiple LDAP-authenticated users at a time, select the LDAP-authenticated users that you want to import and click **Import**.

Modify user information

If the information about a user, such as the mobile phone number or email address, is changed, you must go to the console of the bastion host to which the user is imported to update the information at the earliest opportunity. Otherwise, the user may not receive verification codes and cannot log on to the bastion host. If the mobile phone number of the user is changed and is not updated in the bastion host in a timely manner, the user cannot log on to the bastion host because verification codes are sent to the previous mobile phone number.

> **Note** You can modify the information only about local users, AD-authenticated users, and LDAP-authenticated users. You cannot modify the information about RAM users. For more information about how to modify the information about RAM users, see Modify the basic information about a RAM user.

1.
2.
3. Find the user whose information you want to modify and click the username.
4. On the **Basic Info** tab, modify the user information and click **Update**.

Lock or unlock a user

If a user no longer needs a bastion host to perform O&M operations within a specific period of time, you can lock the user on the Users page. The locked user can no longer log on to or perform O&M operations on the hosts on which the user is granted permissions. If a locked user needs to perform O&M operations, you can unlock the user.

1.
2.
3. On the **Users** page, select the user that you want to lock or unlock and then click **Lock** or **Unlock**.

   > **Notice** The locking or unlocking operation immediately takes effect. Proceed with caution.

   The following list describes the locking and unlocking operations:

   - **Lock**: After the user is locked, the user can no longer log on to or perform O&M operations on the hosts on which the user is granted permissions. In the **Status** column of the user in the user list, the status changes from **Normal** to **Locked**. After the user is locked, you can still modify the basic information about the user, and authorize the user to manage specific hosts and host groups.
   - **Unlock**: After you unlock the user, the system sends you the message **Unlock successfully**. This indicates that the user is unlocked. The unlocked user can log on to or perform O&M operations on the hosts on which the user is granted permissions.

Host the public key of a user

You can configure a public key for a user to host the public key on a bastion host. Then, the user can use a private key to log on to the bastion host from an O&M client.

1.
2.
3. In the user list, click the username of the user for which you want to configure a public key. On the **User Details** page, click the **User Public Key** tab and click **Add SSH Public Key**.
4. In the **Add SSH Public Key** panel, configure the **Public Key Name**, **Public Key**, and **Remarks** parameters.

5. Click **Add SSH Public Key**.

   After you configure the public key, the public key is hosted on the bastion host. You can view the public key in the public key list.

Delete a user

If a user no longer needs to perform O&M operations on hosts by using a bastion host, you can delete the user to reduce security risks.

1.
2.
3. In the user list, select the user that you want to delete and click **Delete**.

1.5.1.2. Modify user information

If the information about a user in a bastion host, such as the mobile phone number of a user, is changed, you must go to the Bastionhost console to update the information at the earliest opportunity. This topic describes how to modify user information in the Bastionhost console.

Context

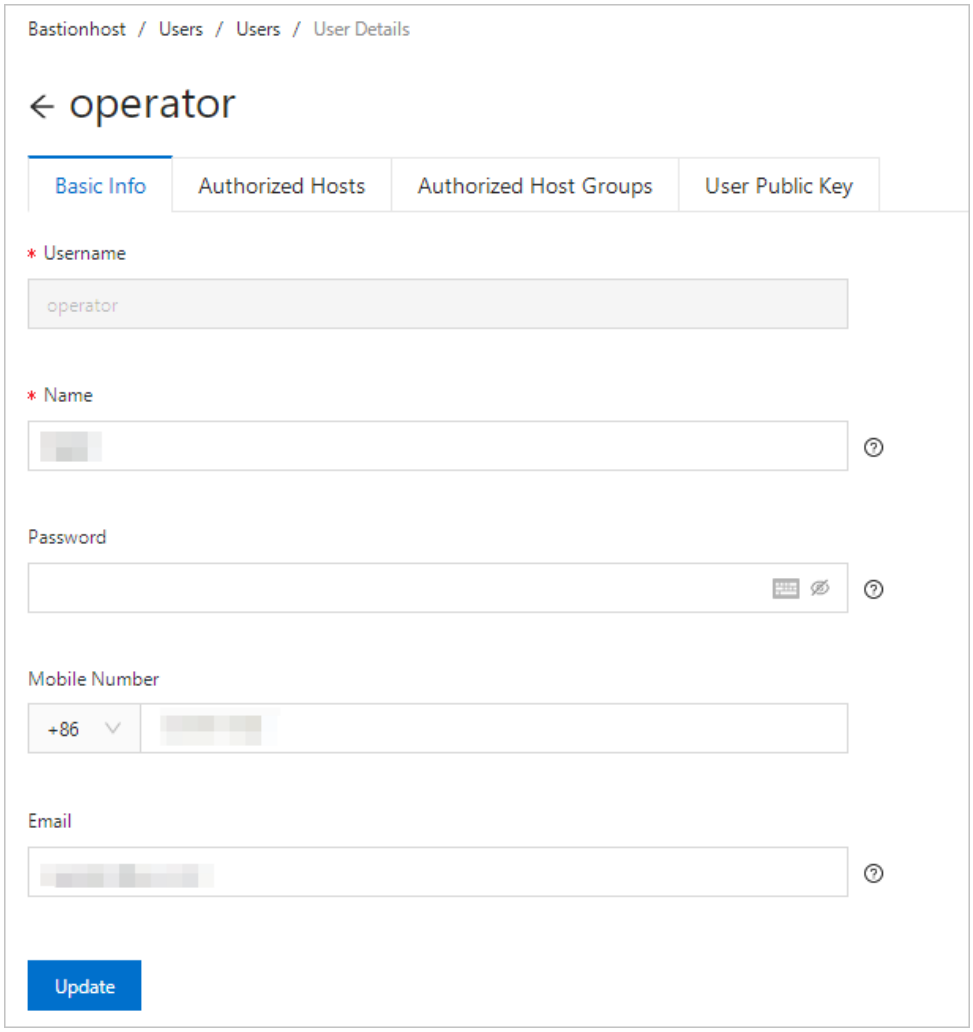
If the information about a user in a bastion host, such as the mobile phone number of a user, is changed and is not updated in the bastion host in a timely manner, the user cannot log on to the bastion host. This is because verification codes are sent to the previous mobile phone number. Therefore, if user information, such as the mobile phone number or email address, is changed, you must go to the Bastionhost console to update the information at the earliest opportunity.

Limits

You can modify the information only about local users, Active Directory (AD)-authenticated users, and Lightweight Directory Access Protocol (LDAP)-authenticated users. You cannot modify the information about Resource Access Management (RAM) users. For more information about how to modify the information about RAM users., see Modify the basic information about a RAM user.

Procedure

1.
2.
3. Find the user whose information you want to modify and click the username.
4. On the **Basic Info** tab, modify the information such as **Password**, **Mobile Number**, **Email**, and **User Group**.



> **Note** If two-factor authentication is enabled for the user, make sure that you enter a valid mobile phone number. Otherwise, the user cannot receive a verification code for logon For more information about countries and areas where SMS-based two-factor authentication is supported, see Supported countries and areas for SMS-based two-factor authentication.

5. Click **Update**.

1.5.1.3. Lock or unlock a user

If a user no longer needs a bastion host to perform O&M operations within a specific period of time, you can lock the user on the Users page. The locked user cannot log on to the required host to perform O&M operations. If a locked user needs to perform O&M operations again, you can unlock the user. This topic describes how to lock and unlock a user.

Procedure

1.
2.
3. On the **Users** page, select the user that you want to lock or unlock.

   You can select more than one user at a time.

4. Notice The locking or unlocking operation immediately takes effect. Proceed with caution.

   Click **Lock** or **Unlock**.

   The following list describes the locking and unlocking operations:

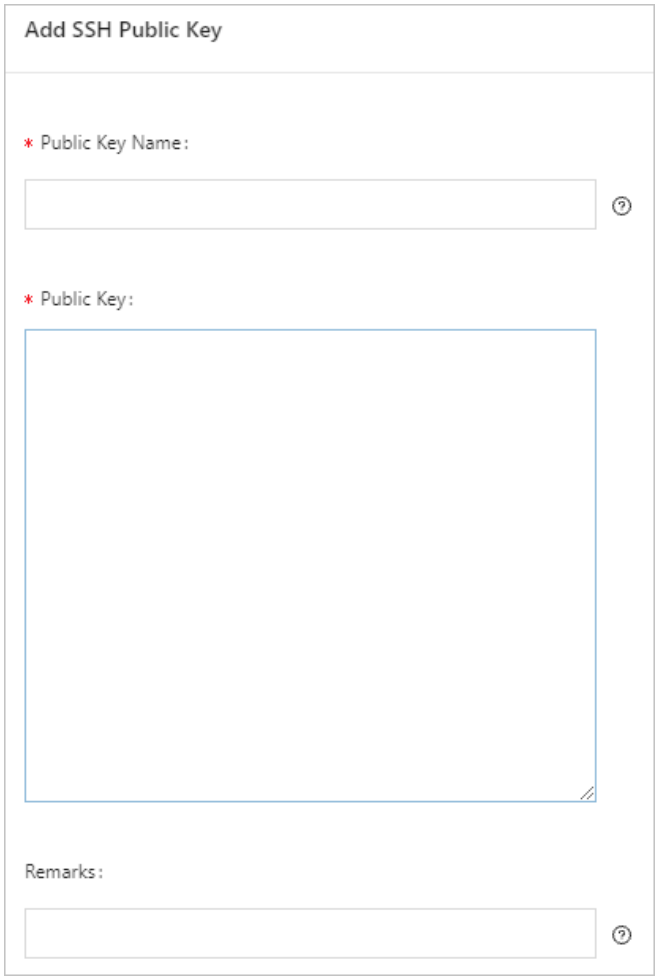
   - **Lock**: After the user is locked, the user cannot log on to the authorized hosts to perform O&M operations, and the status of the user changes from Normal to Locked. After the user is locked, you can still modify the basic information of the user, and authorize hosts and host groups for the user.
   - **Unlock**: After the user is unlocked, the system prompts that the user is unlocked. The user can log on to the authorized hosts to perform O&M operations.

1.5.1.4. Host the public key of a user

After you configure a public key, the public key is hosted on Bastionhost. You can use the private key to log on to a bastion host from an O&M client. This topic describes how to host a public key on Bastionhost.

Procedure

1.
2.
3. In the user list, click the name of a user for which you want to configure a public key.
4. On the **User Details** page, click the **User Public Key** tab.
5. Click **Add SSH Public Key**.
6. In the **Add SSH Public Key** panel, configure the following parameters.



Parameter	Description
Public Key Name	Specify the name of the public key.
Public Key	Enter the public key.
Remarks	Enter the description of the public key.

7. Click **Add SSH Public Key**.

   After you configure the public key, the public key is hosted on Bastionhost. You can view the public key in the public key list.

Result

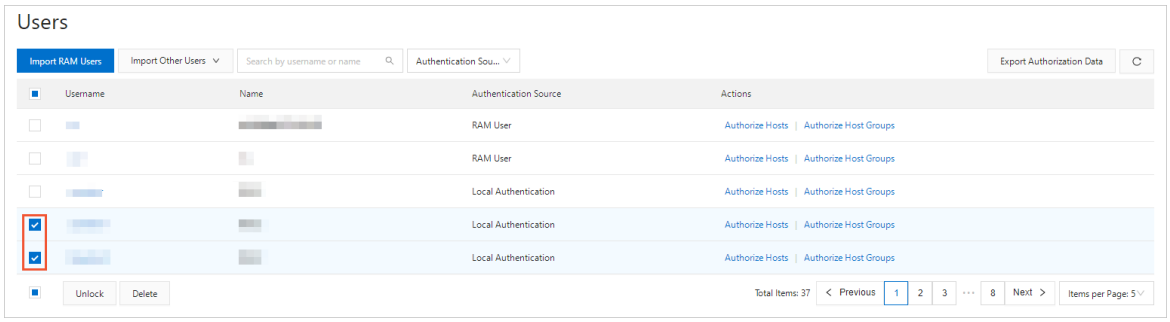
After the public key is hosted on Bastionhost, you can use the private key to log on to the bastion host from an O&M client. For more information, see SSH-based O&M.

1.5.1.5. Delete users

This topic describes how to delete users. Deleting users that no longer need to perform O&M operations on hosts reduces security risks.

Procedure

1.
2.
3. On the Users page, select the users you want to delete.



4. Click **Delete**.

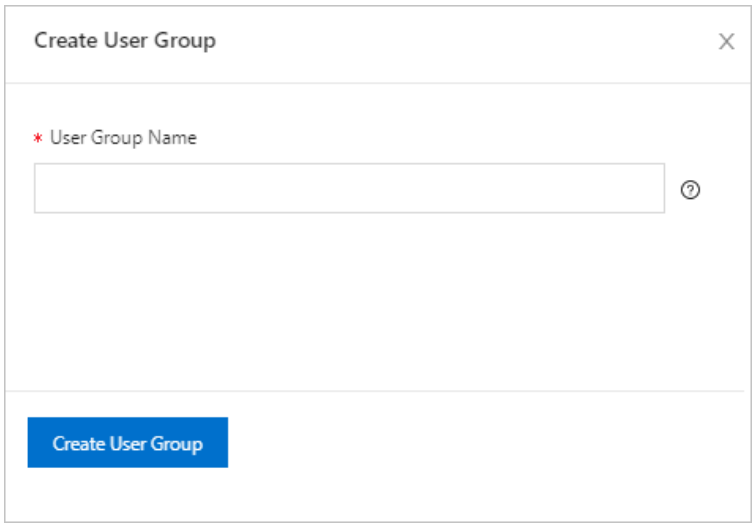
1.5.2. User group management

1.5.2.1. Create a user group

You can add multiple users to a user group to manage and authorize them in a centralized manner. This topic describes how to create a user group.

Procedure

1.
2.
3.
4. In the Create User Group pane, enter a user group name in the **User Group Name** field.



> **Note** We recommend that you specify a meaningful user group name to facilitate subsequent management and maintenance.

5. Click **Create User Group**.

Result

The created user group is displayed on the User Groups page.

What's next

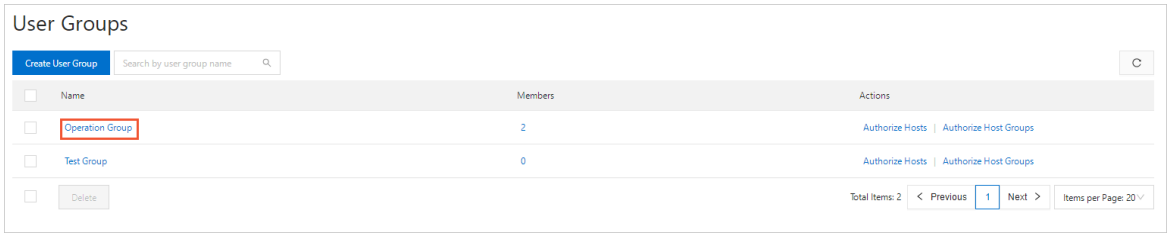
After you create a user group, you can add users to the user group. For more information, see Add or remove users to or from a user group.

1.5.2.2. Modify the information of a user group and delete user groups

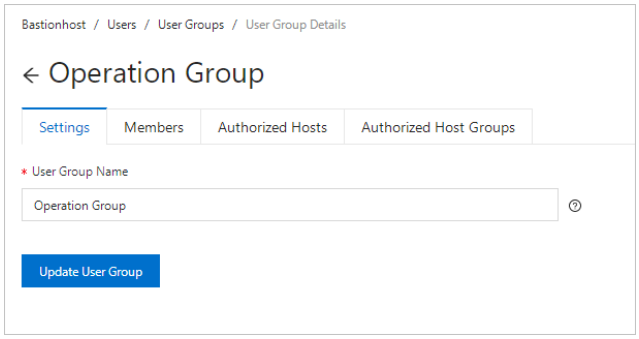
This topic describes how to modify the information of a user group and delete user groups.

Modify the information of a user group

1.
2.
3. On the User Groups page, click the name of the user group whose information you want to modify.



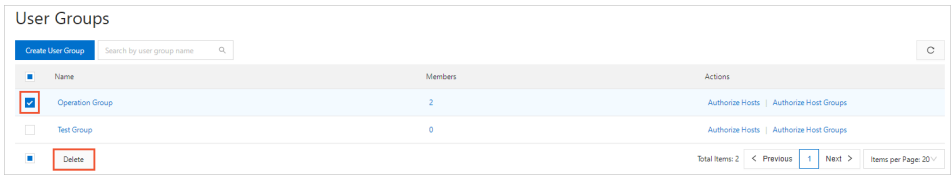
4. Enter a new name for the user group in the **User Group Name** field.



5. Click **Update User Group**.

Delete user groups

1.
2.
3. On the User Groups page, select the user groups that you want to delete, and click **Delete**.

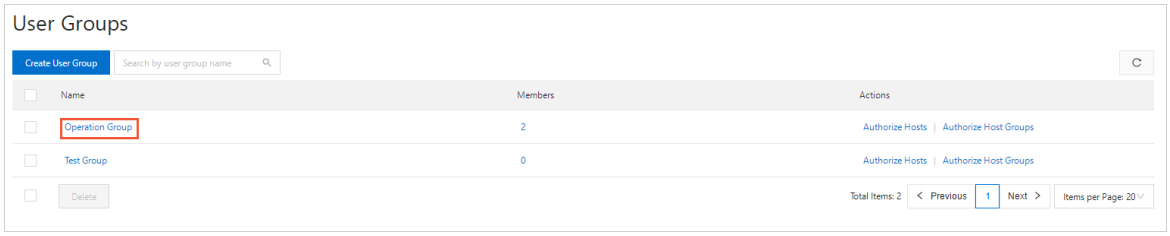


1.5.2.3. Add or remove users to or from a user group

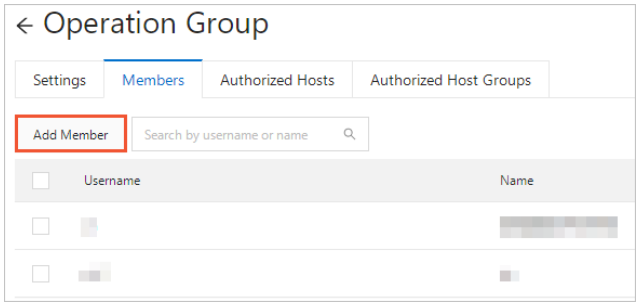
This topic describes how to add or remove users to or from a user group. After you add users to a user group, you can authorize the users at a time.

Add users to a user group

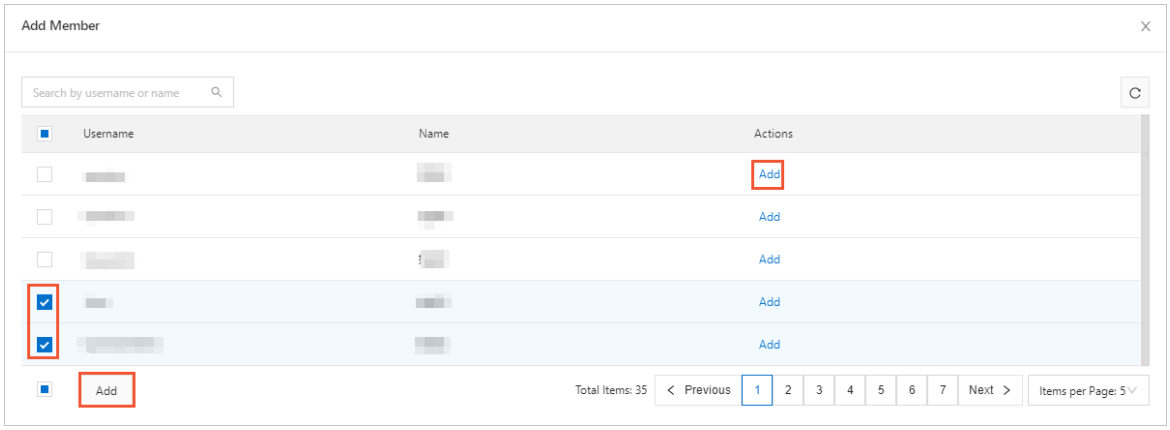
1.
2.
3. On the User Groups page, click the name of the user group to which you want to add users.



4. Click the **Members** tab.
5. Click **Add Member**.



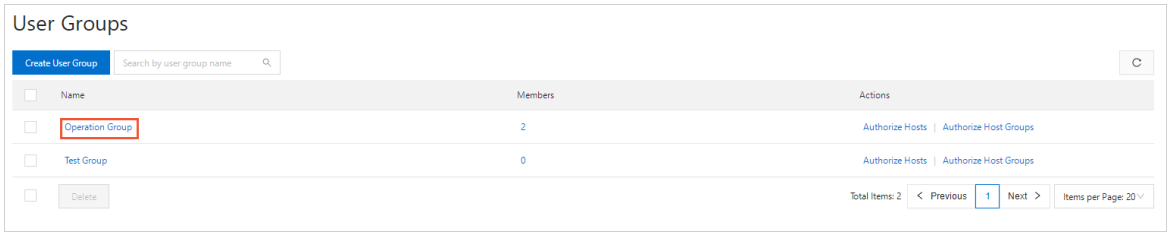
6. In the **Add Member** dialog box, select the users you want to add and click **Add** in the lower-left corner.



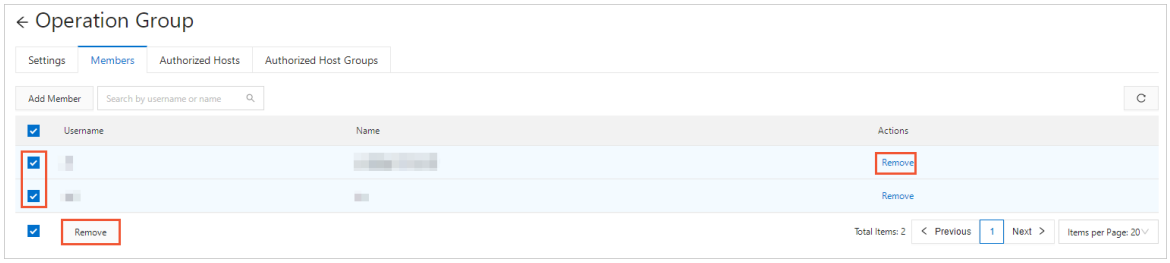
> **Note** To add a single user, click **Add** in the **Actions** column. In the message that appears, click Add.

Remove users from a user group

1.
2.
3. On the User Groups page, click the name of the user group to which you want to add users.



4. Click the **Members** tab.
5. Select the users you want to remove and click **Remove** in the lower-left corner.



> **Note** To remove a single user, click **Remove** in the **Actions** column. In the message that appears, click Remove.

1.5.3. Host authorization

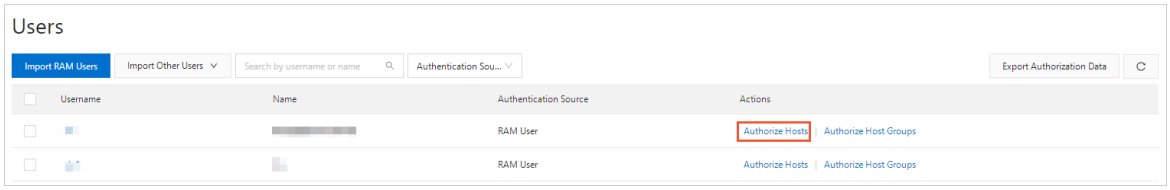
1.5.3.1. Authorize a user to manage hosts

Bastionhost allows you to authorize a user to manage hosts. After you add a user, you can authorize the user to manage hosts. After the user is authorized to manage the hosts, the user can log on to a bastion host to perform O&M operations on the hosts. This topic describes how to authorize a user to manage hosts.

Authorize a user to manage hosts

To authorize a user to manage hosts, perform the following steps:

1.
2.
3. Find the user whom you want to authorize to manage hosts and click **Authorize Hosts** in the **Actions** column.

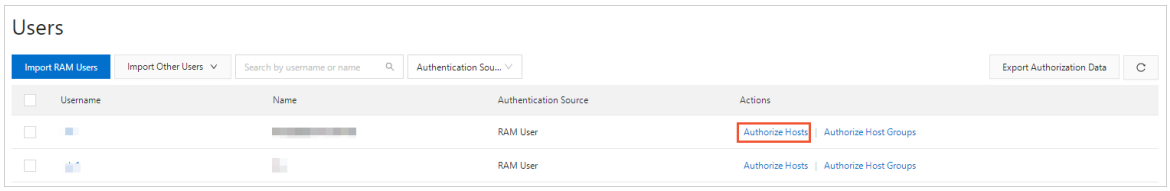


4. On the **Authorized Hosts** tab, click **Authorize Hosts**.
5. In the Authorize Hosts panel, select one or more hosts you want to authorize the user to manage and click **OK**.

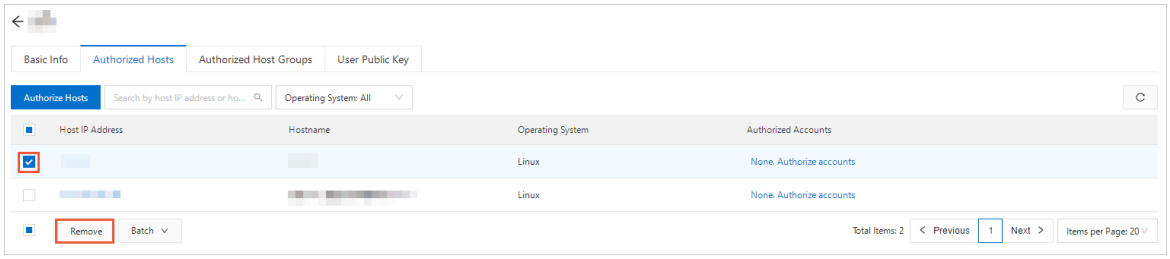
Remove the hosts that a user is authorized to manage

If a user is no longer required to manage specific hosts, perform the following steps to remove the hosts that the user is authorized to manage to achieve the principle of least privilege:

1.
2.
3. Find the user and click **Authorize Hosts** in the **Actions** column.



4. Select the hosts that you want to remove and click **Remove**.

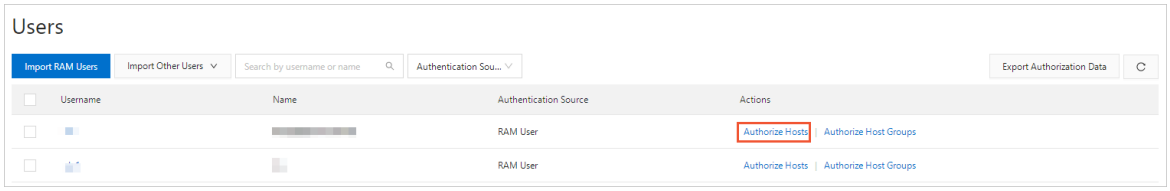


5. In the message that appears, click **Remove**.

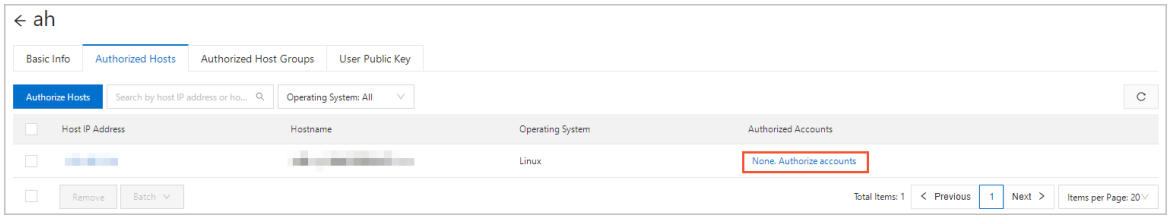
Authorize the accounts of a single host for a user

To authorize the accounts of a single host for a user, perform the following steps:

1.
2.
3. Find the user whom you want to authorize to manage hosts and click **Authorize Hosts** in the **Actions** column.



4. On the **Authorized Hosts** tab, click the account name or **None. Authorize accounts** in the **Authorized Accounts** column.



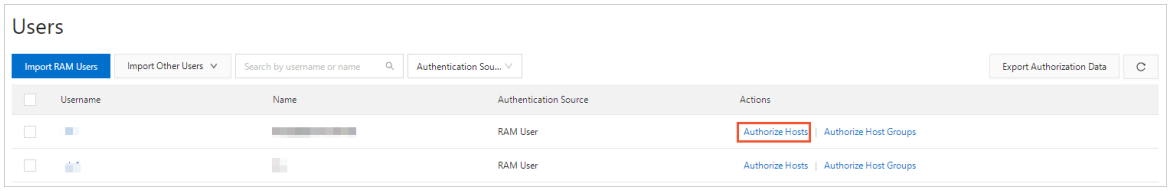
5. In the Select Accounts panel, select one or more accounts and click **Update**.

> **Note** If no account is created on the host, you can click **Create Host Account** in the Select Accounts panel to create an account.

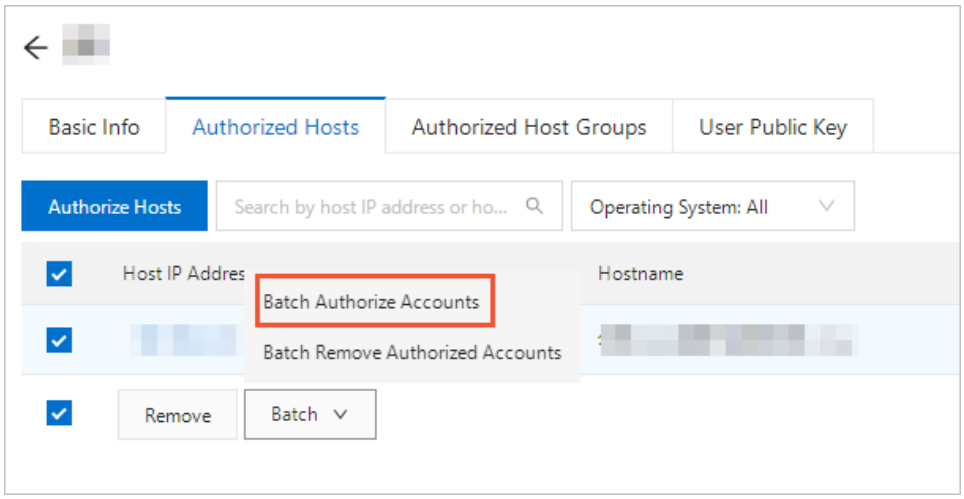
Authorize the accounts of multiple hosts for a user

To authorize the accounts of multiple hosts for a user at a time, perform the following steps:

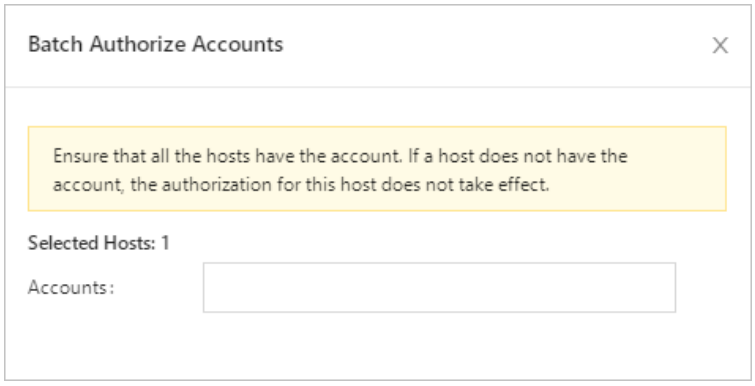
1.
2.
3. Find the user whom you want to authorize to manage hosts and click **Authorize Hosts** in the **Actions** column.



4. On the Authorized Hosts tab, select the hosts whose accounts you want to authorize for the user and choose **Batch > Batch Authorize Accounts**.



5. In the Batch Authorize Accounts panel, specify **Accounts**.



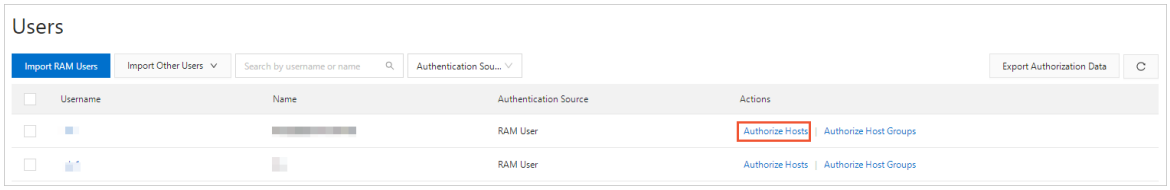
> **Note** When you want to authorize the accounts of multiple hosts for a user at a time, you can select only one host account at a time.

6. Click **Update**.

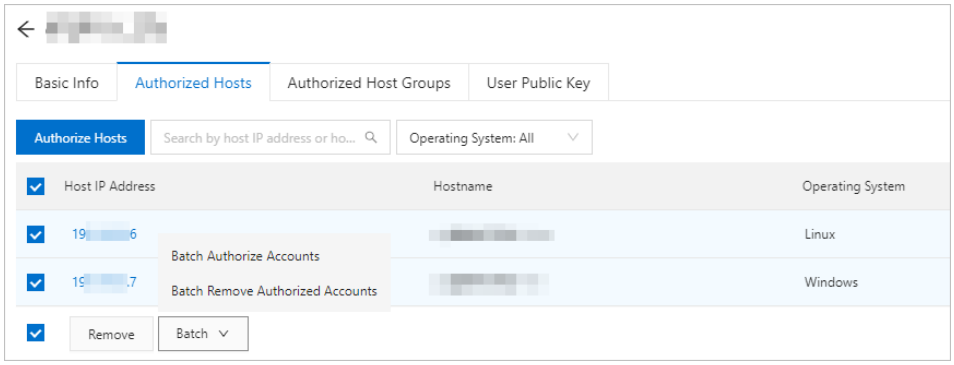
Remove the accounts of multiple hosts that are authorized for a user

To remove the accounts of multiple hosts that are authorized for a user at a time, perform the following steps:

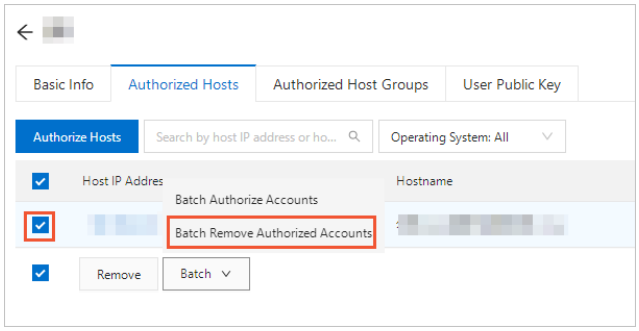
1.
2.
3. Find the user from whom you want to remove the accounts of multiple hosts and click **Authorize Hosts** in the **Actions** column.



4. On the **Authorized Hosts** tab, select the hosts.
5. Choose **Batch > Batch Remove Authorized Accounts**.



6. In the Batch Remove Authorized Accounts panel, specify Accounts.



> **Note** When you remove the accounts of multiple hosts that are authorized for a user at a time, you can select only one host account at a time.

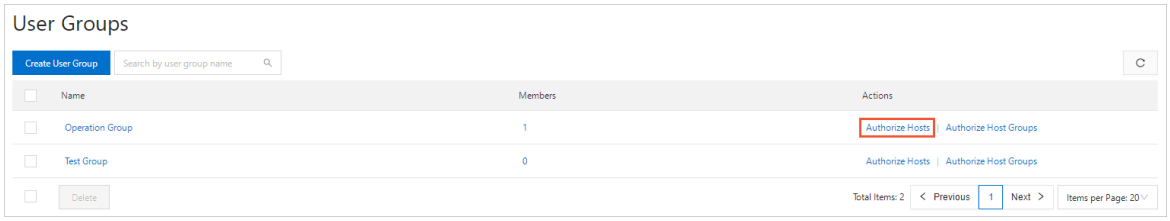
7. Click **Update**.

1.5.3.2. Authorize a user group to manage hosts

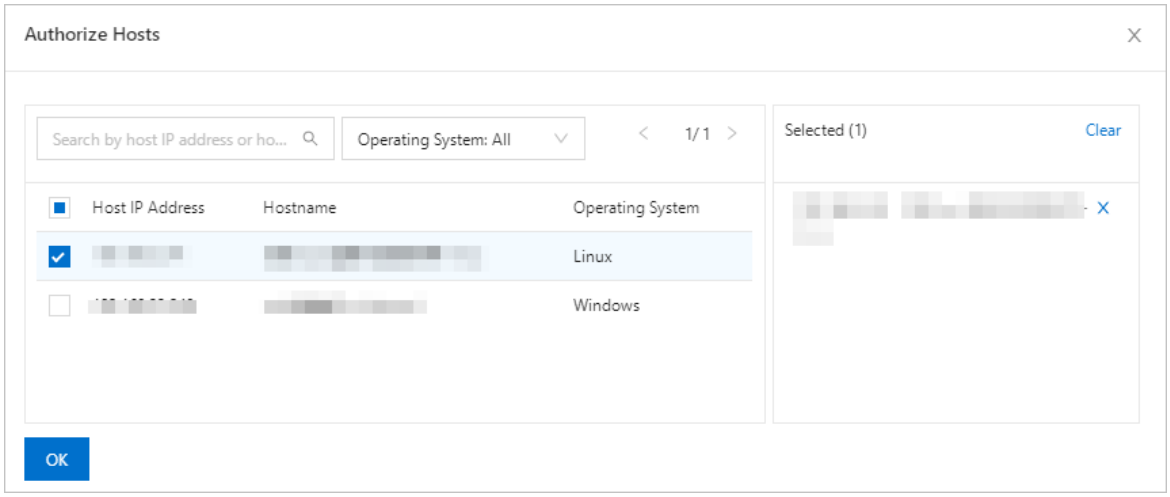
Bastionhost allows you to authorize a user group to manage hosts. After you create a user group, you can authorize the user group to manage hosts. After the users group is authorized to manage the hosts, the users in the user group can log on to a bastion host to perform O&M operations on the hosts. This topic describes how to authorize a user group to manage hosts.

Authorize a user group to manage hosts

1.
2.
3. Find the user group that you want to authorize to manage hosts and click **Authorize Hosts** in the **Actions** column.



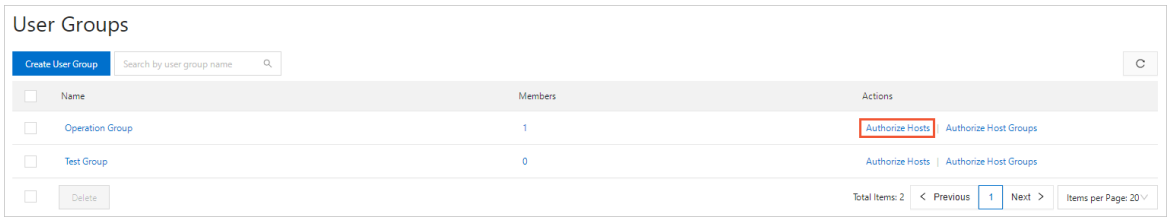
4. On the **Authorized Hosts** tab, click **Authorize Hosts**.
5. In the **Authorize Hosts** panel, select one or more hosts that you want to authorize for the user group to manage and click **OK**.



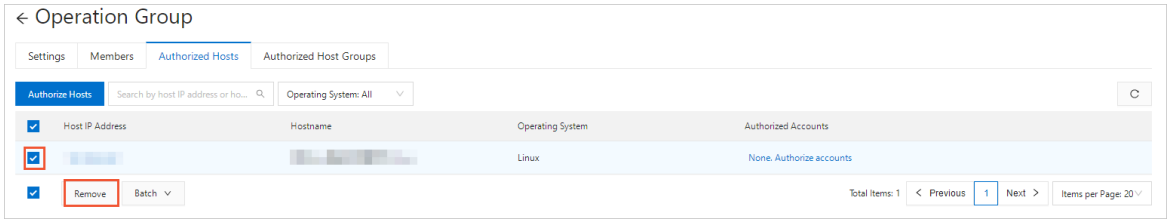
Remove the hosts that a user group is authorized to manage

If a user group is no longer required to manage specific hosts, perform the following steps to remove the hosts that the user group is authorized to manage to achieve the principle of least privilege:

1.
2.
3. Find the user group and click **Authorize Hosts** in the **Actions** column.



4. On the Authorized Hosts tab, select the hosts that you want to remove and click **Remove**.

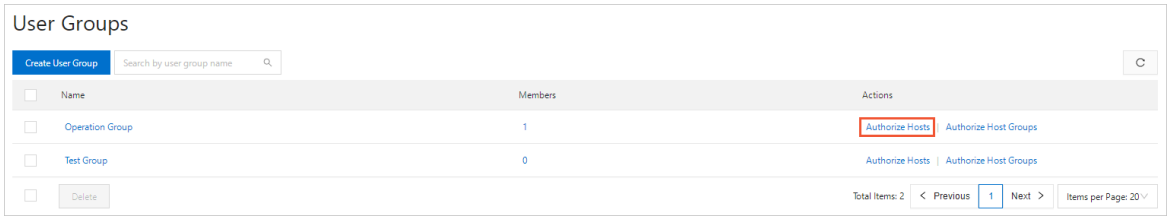


5. In the message that appears, click **Remove**.

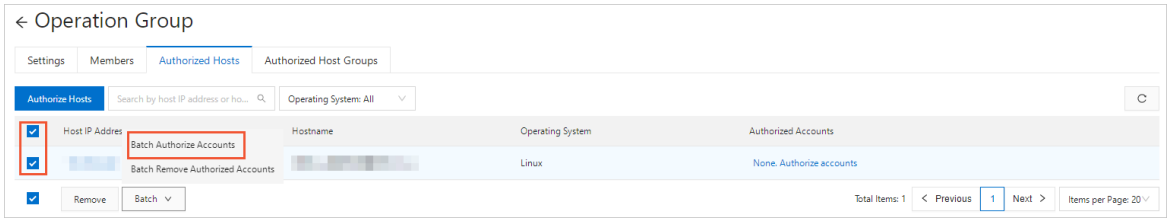
Authorize the accounts of multiple hosts for a user group

To authorize the accounts of multiple hosts for a user group at a time, perform the following steps:

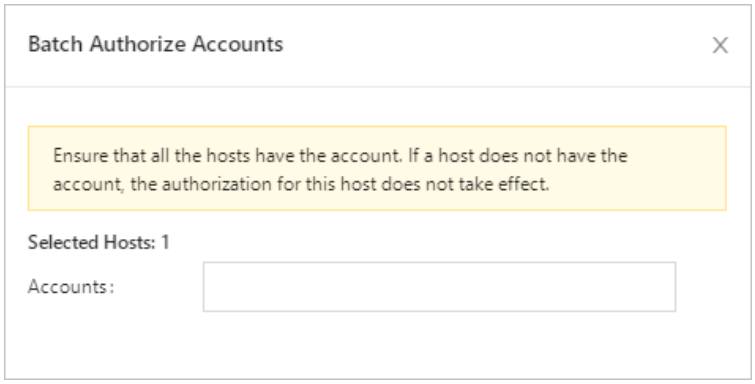
1.
2.
3. Find the user group that you want to authorize to manage hosts and click **Authorize Hosts** in the **Actions** column.



4. On the Authorized Hosts tab, select the hosts whose accounts you want to authorize for the user and choose **Batch > Batch Authorize Accounts**.



5. In the Batch Authorize Accounts panel, specify **Accounts**.



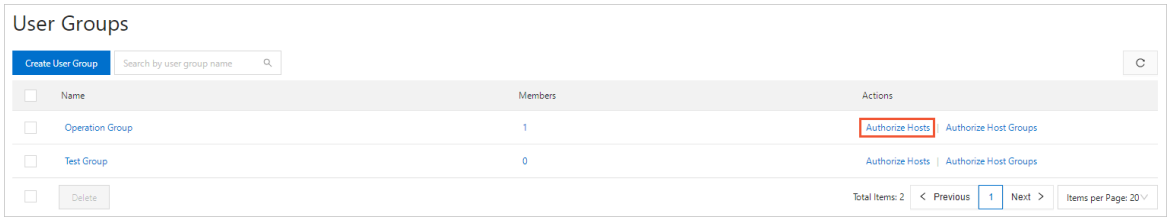
> **Note** When you want to authorize the accounts of multiple hosts for a user at a time, you can select only one host account at a time.

6. Click **Update**.

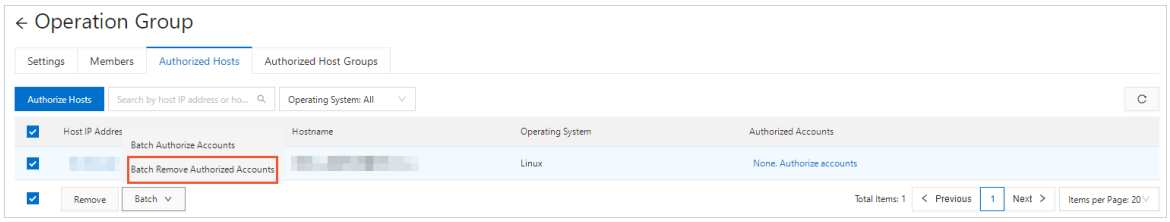
Remove the accounts of multiple hosts that are authorized for a user group

To remove the accounts of multiple hosts that are authorized for a user group at a time, perform the following steps:

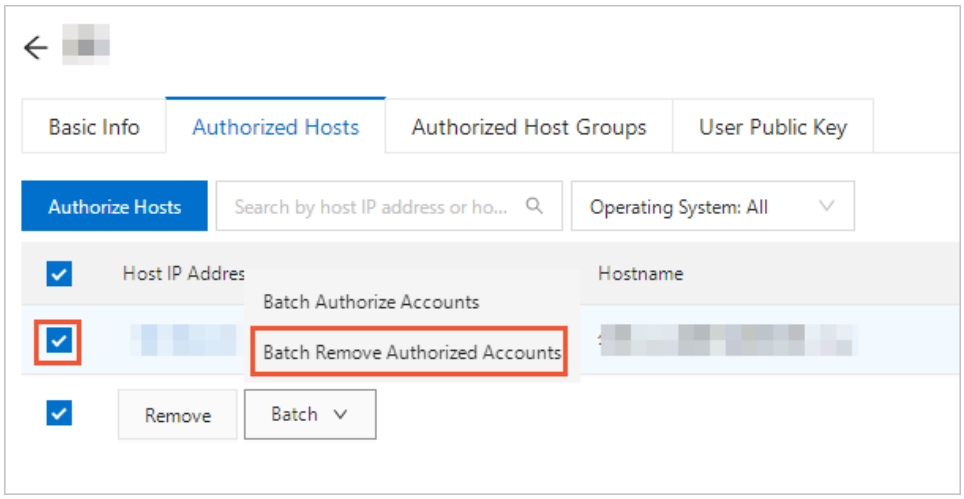
1.
2.
3. Find the user group and click **Authorize Hosts** in the **Actions** column.



4. On the **Authorized Hosts** tab, select the hosts whose accounts you want to remove and choose **Batch > Batch Remove Authorized Accounts**.



5. In the Batch Remove Authorized Accounts panel, specify **Accounts**.



> **Note** When you remove the accounts of multiple hosts that are authorized for a user at a time, you can select only one host account at a time.

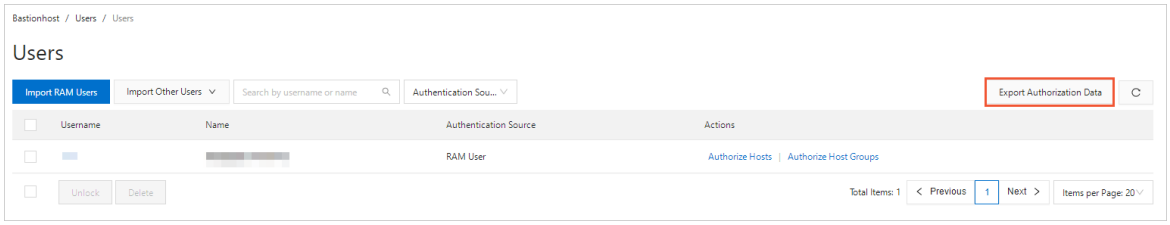
6. Click **Update**.

1.5.3.3. Export authorization data

The Bastionhost console allows you to export authorization data. You can analyze this data to identify the relationship between all users and hosts or host groups. This topic describes how to export the authorization data.

Procedure

1.
2.
3. On the **Users** page that appears, click **Export Authorization Data** in the upper-right corner.



The authorization data is exported to a *CSV* file in your local machine.

1.5.4. Host group authorization

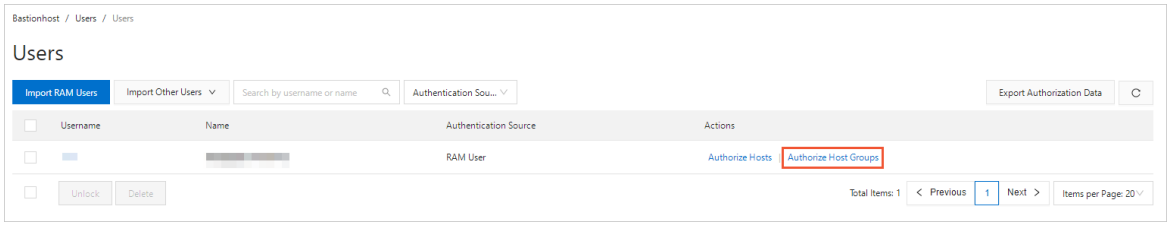
1.5.4.1. Authorize a user to manage host groups

Bastionhost allows you to authorize a user to manage host groups. After you add a user, you can authorize the user to manage host groups. After the host groups are authorized for the user to manage, the user can log on to a bastion host to perform O&M operations on the hosts in the host groups. This topic describes how to authorize a user to manage host groups.

Authorize a user to manage host groups

To authorize a user to manage host groups, perform the following steps:

1.
2.
3. Find the user group that you want to authorize to manage host groups and click **Authorize Host Groups** in the **Actions** column.

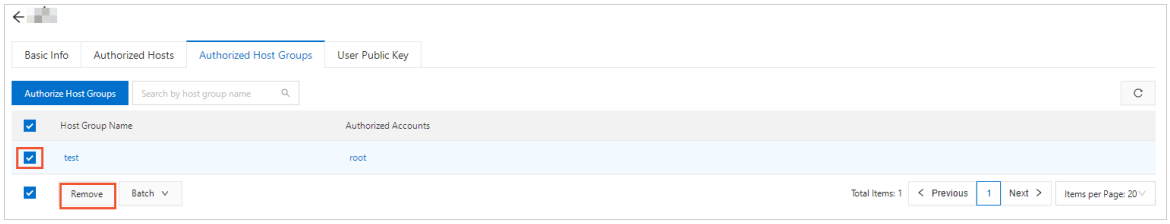


4. On the **Authorized Host Groups** tab, click **Authorize Host Groups**.
5. In the Authorize Host Groups panel, select one or more host groups that you want to authorize for the user to manage and click **OK**.

Remove the host groups that a user is authorized to manage

If a user is no longer required to manage specific host groups, perform the following steps to remove the host groups that the user is authorized to manage to achieve the principle of least privilege:

1.
2.
3. Find the user and click **Authorize Host Groups** in the **Actions** column.
4. Select the host groups that you want to remove and click **Remove**.

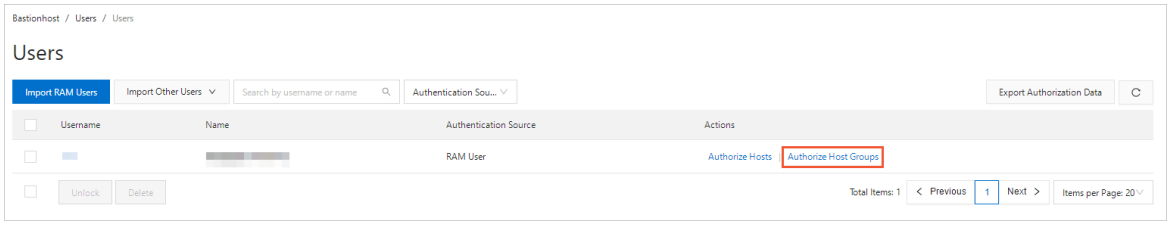


5. In the message that appears, click **Remove**.

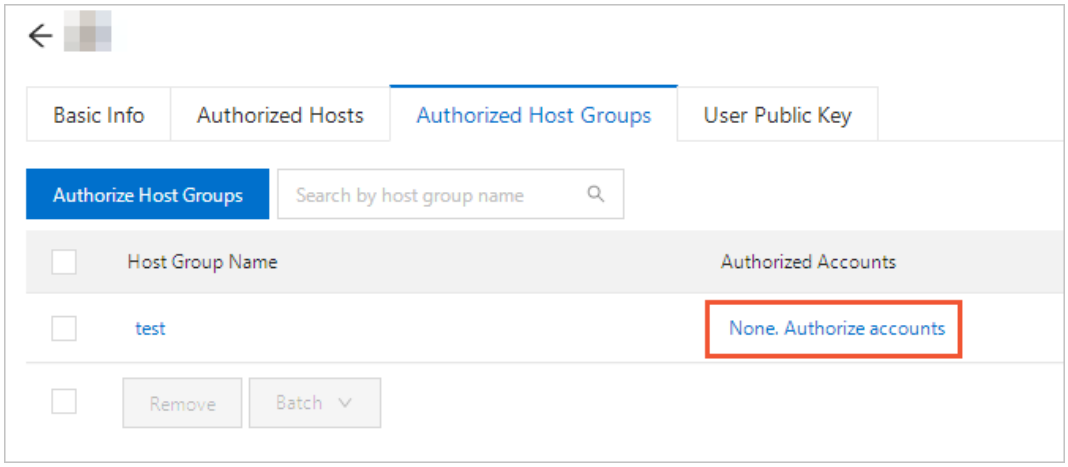
Authorize the accounts of a single host group for a user

To authorize the accounts of a single host group for a user group, perform the following steps:

1.
2.
3. Find the user group that you want to authorize to manage host groups and click **Authorize Host Groups** in the **Actions** column.

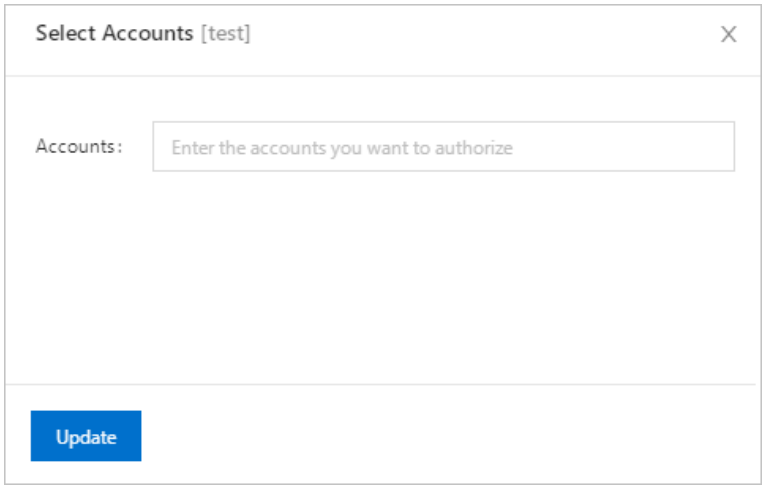


4. On the **Authorized Host Groups** tab, click **None. Authorize accounts**.



> **Note** If you want to modify the accounts that are authorized for the user, you can click the account name in the **Authorized Accounts** column and specify the Accounts parameter.

5. In the Select Accounts panel, specify **Accounts**.

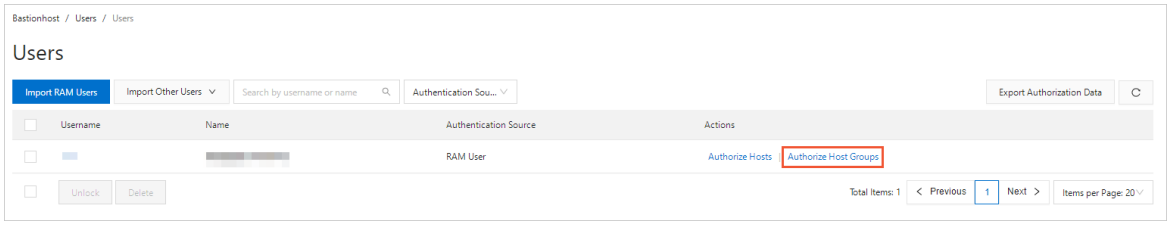


6. Click **Update**.

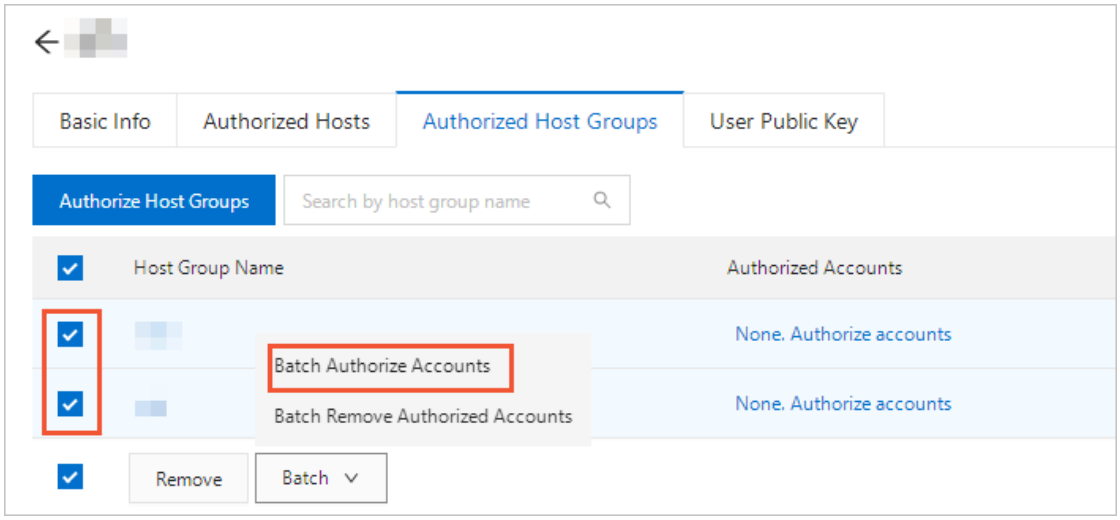
Authorize the accounts of multiple host groups for a user

To authorize the accounts of multiple host groups for a user at a time, perform the following steps:

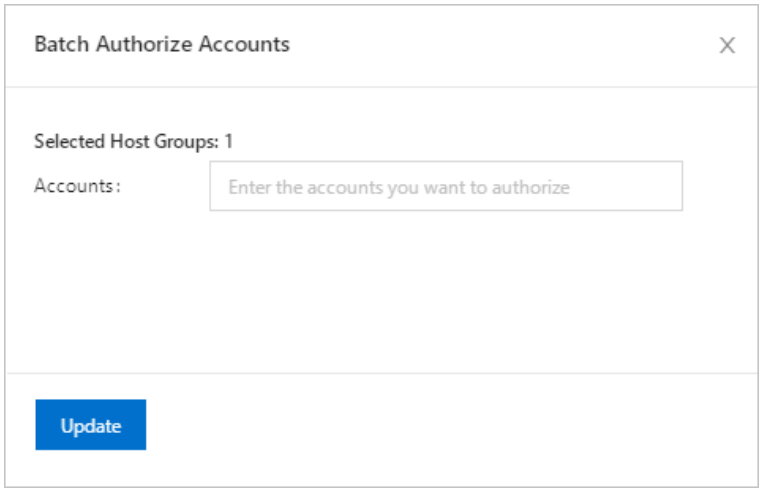
1.
2.
3. Find the user group that you want to authorize to manage host groups and click **Authorize Host Groups** in the **Actions** column.



4. On the Authorized Host Groups tab, select the host groups whose accounts you want to authorize for the user and choose **Batch > Batch Authorize Accounts**.



5. In the Batch Authorize Accounts panel, specify **Accounts**.

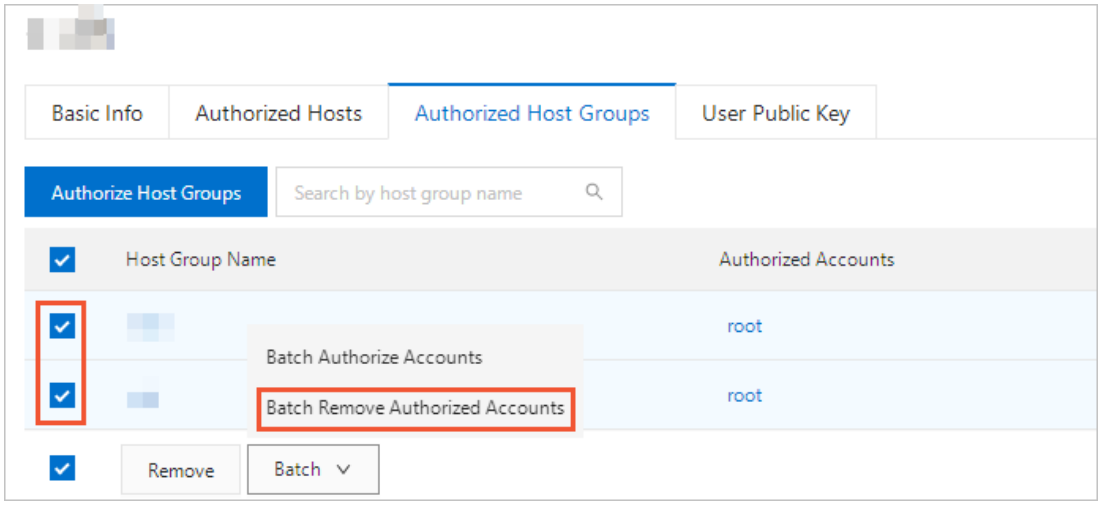


6. Click **Update**.

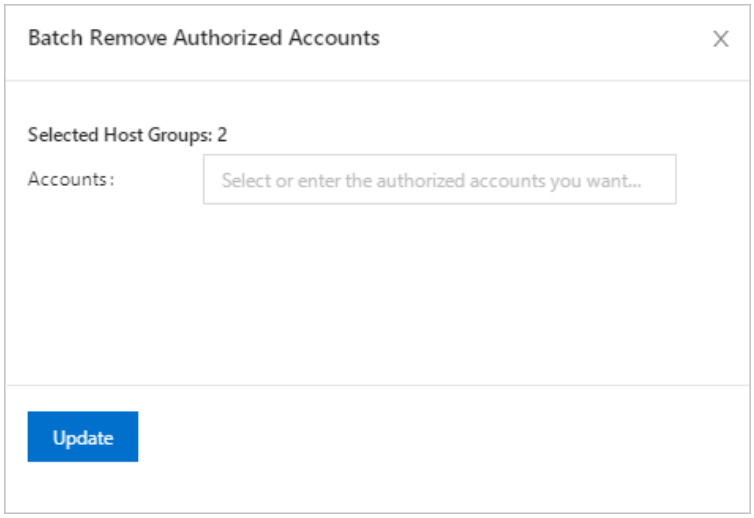
Remove the accounts of multiple host groups that are authorized for a user

To remove the accounts of multiple host groups that are authorized for a user at a time, perform the following steps:

1.
2.
3. Find the user from whom you want to remove the accounts of multiple host groups and click **Authorize Host Groups** in the **Actions** column.
4. On the **Authorized Host Groups** tab, select the host groups and choose **Batch > Batch Remove Authorized Accounts**.



5. In the Batch Remove Authorized Accounts panel, specify **Accounts**.



6. Click **Update**.

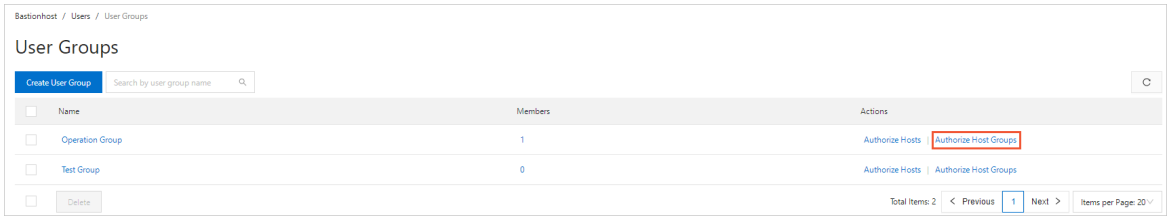
1.5.4.2. Authorize a user group to manage host groups

Bastionhost allows you to authorize a user group to manage host groups. After you create a user group, you can authorize the user group to manage host groups. After the host groups are authorized for the user group, the users in the user group can log on to a bastion host to perform O&M operations on the hosts in the host groups. This topic describes how to authorize a user group to manage host groups.

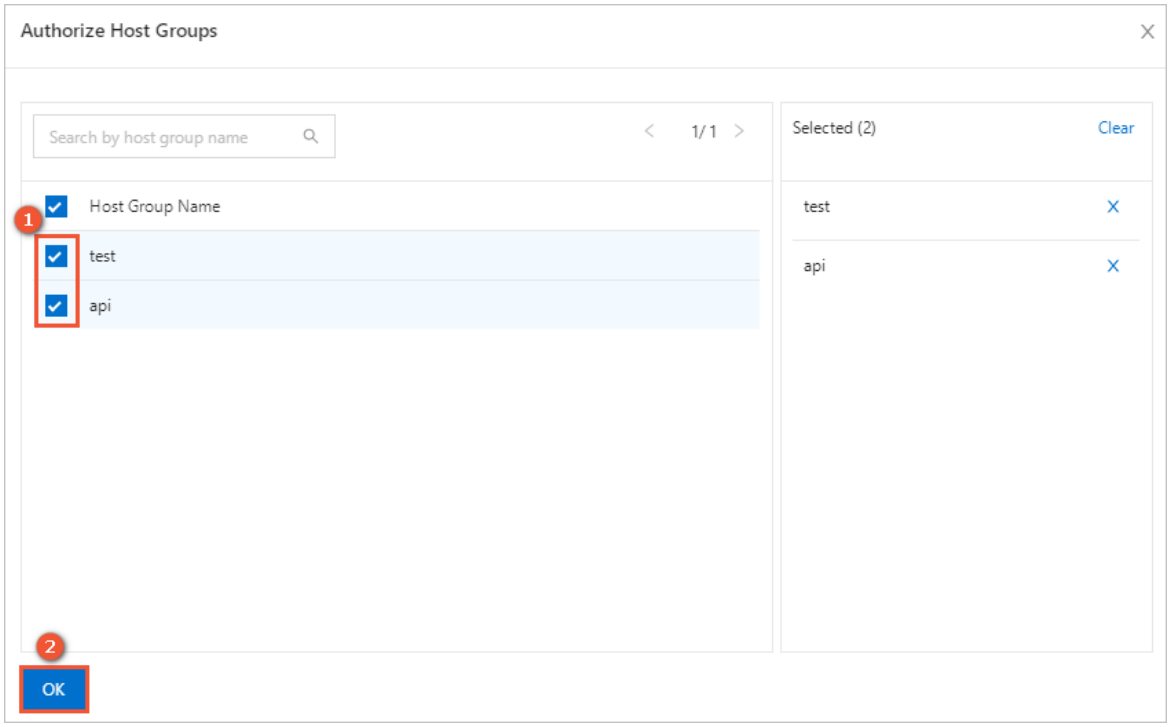
Authorize a user group to manage host groups

To authorize host groups for a user group, perform the following steps:

1.
2.
3. Find the user group that you want to authorize to manage host groups and click **Authorize Host Groups** in the **Actions** column.



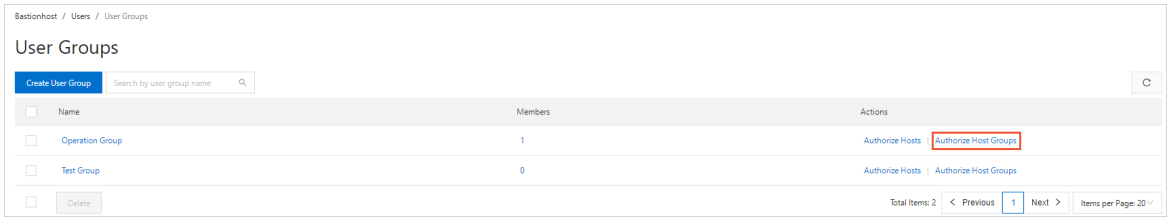
4. On the **Authorized Host Groups** tab, click **Authorize Host Groups**.
5. In the Authorize Host Groups panel, select one or more host groups that you want to authorize for the user group to manage and click **OK**.



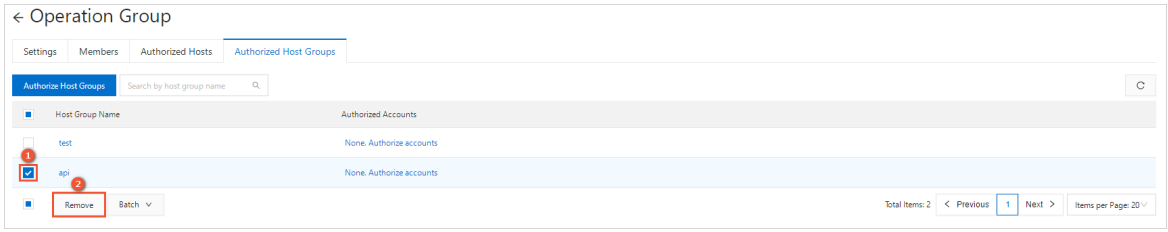
Remove the host groups that a user group is authorized to manage

If a user group is no longer required to manage specific host groups, perform the following steps to remove the host groups that the user group is authorized to manage to achieve the principle of least privilege:

1.
2.
3. Find the user group and click **Authorize Host Groups** in the **Actions** column.



4. On the Authorized Host Groups tab, Select the host groups that you want to remove and click **Remove**.

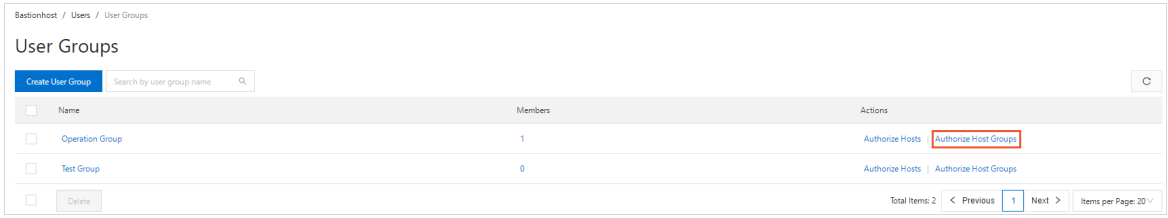


5. In the message that appears, click **Remove**.

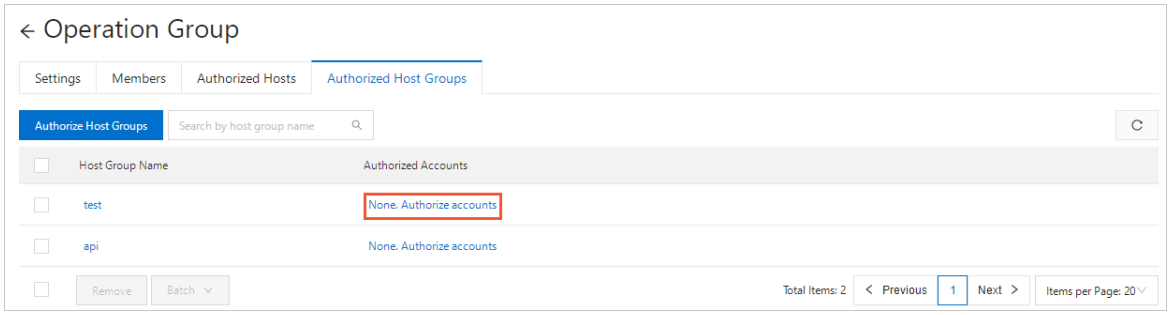
Authorize the accounts of a single host group for a user group

To authorize the accounts of a single host group for a user group, perform the following steps:

1.
2.
3. Find the user group that you want to authorize to manage host groups and click **Authorize Host Groups** in the **Actions** column.



4. On the **Authorized Host Groups** tab, click **None. Authorize accounts.**



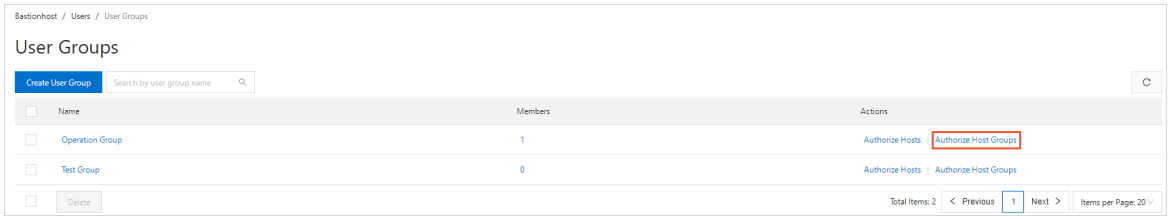
> **Note** If you want to change the accounts that are authorized for the user group, you can click the account name in the **Authorized Accounts** column and specify the Accounts parameter.

5. In the Batch Authorize Accounts panel, specify **Accounts**.
6. Click **Update**.

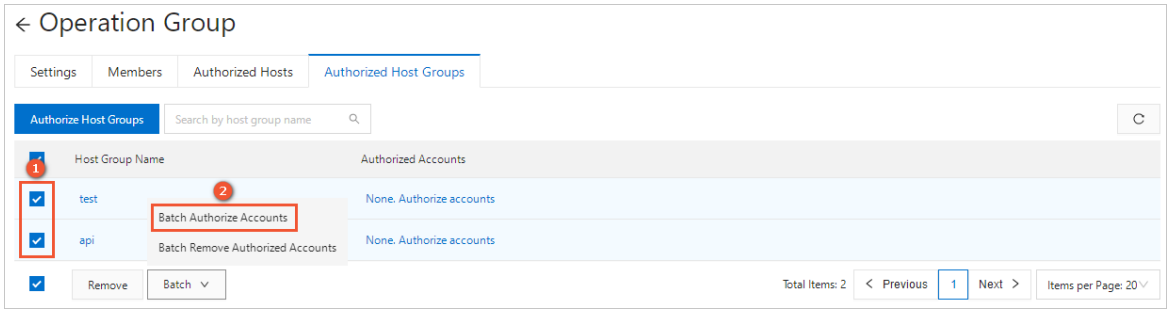
Authorize the accounts of multiple host groups for a user group

To authorize the accounts of multiple host groups for a user group at a time, perform the following steps:

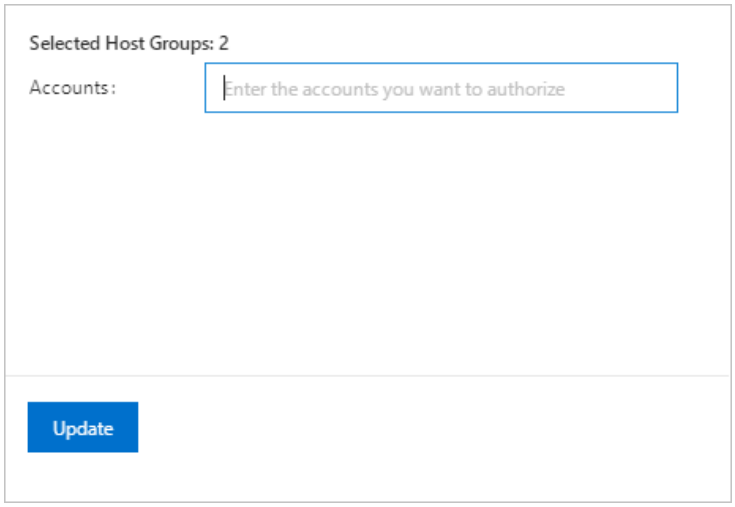
1.
2.
3. Find the user group that you want to authorize to manage host groups and click **Authorize Host Groups** in the **Actions** column.



4. On the Authorized Host Groups tab , select the host groups whose accounts you want to authorize for the user group and choose **Batch > Batch Authorize Accounts**.



5. In the Batch Authorize Accounts panel, specify **Accounts**.

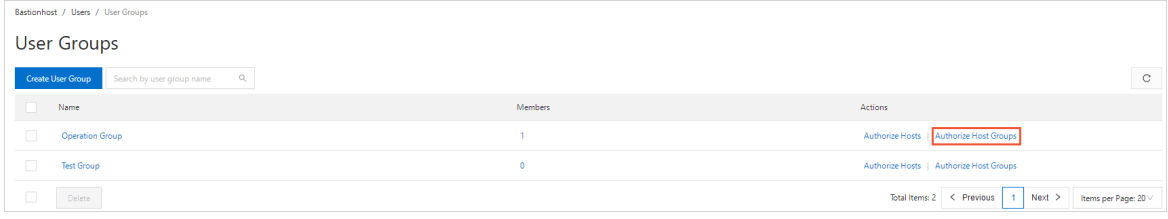


6. Click **Update**.

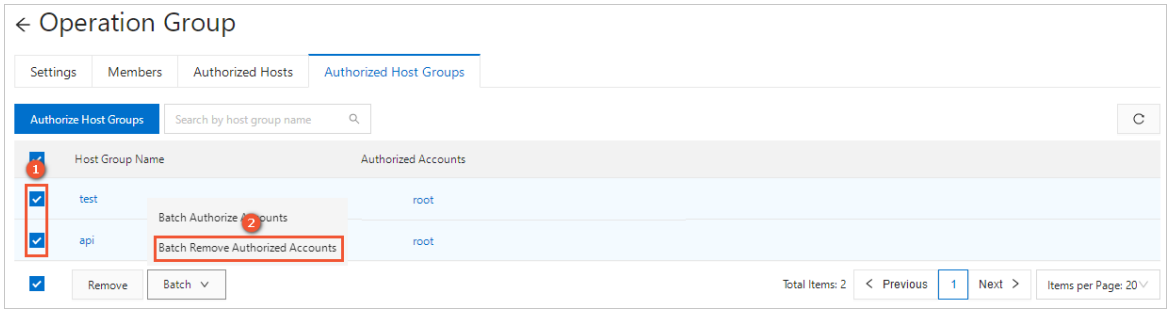
Remove the accounts of multiple host groups that are authorized for a user group

To remove the accounts of multiple host groups that are authorized for a user group at a time, perform the following steps:

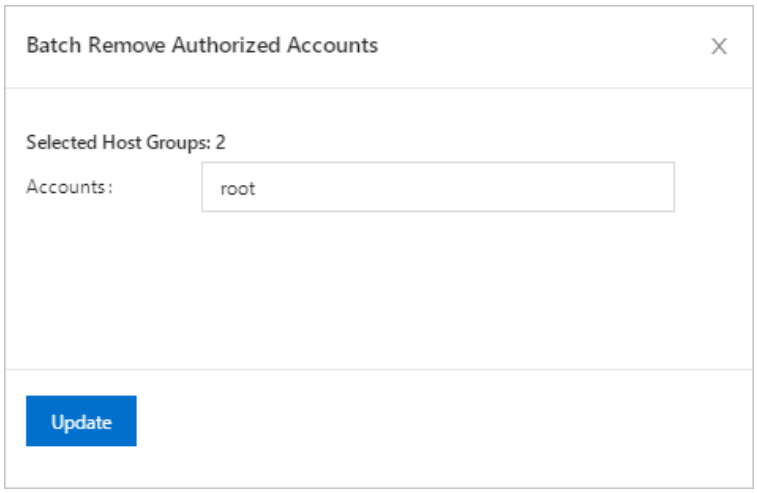
1.
2.
3. Find the user group and click **Authorize Host Groups** in the **Actions** column.



4. On the Authorized Host Groups tab, select the host groups whose accounts you want to remove and choose **Batch > Batch Remove Authorized Accounts**.



5. In the Batch Remove Authorized Accounts panel, specify **Accounts**.



6. Click **Update**.

1.6. Authorization rules

1.6.1. Create an authorization rule

Bastionhost provides the authorization rules feature. The authorization rules feature allows you to authorize multiple users to manage assets at a time. You can also specify a period of time in which the users can access the assets. The feature allows you to manage users and assets in a more efficient manner and control the period of time in which users can access assets. This topic describes how to create an authorization rule.

Context

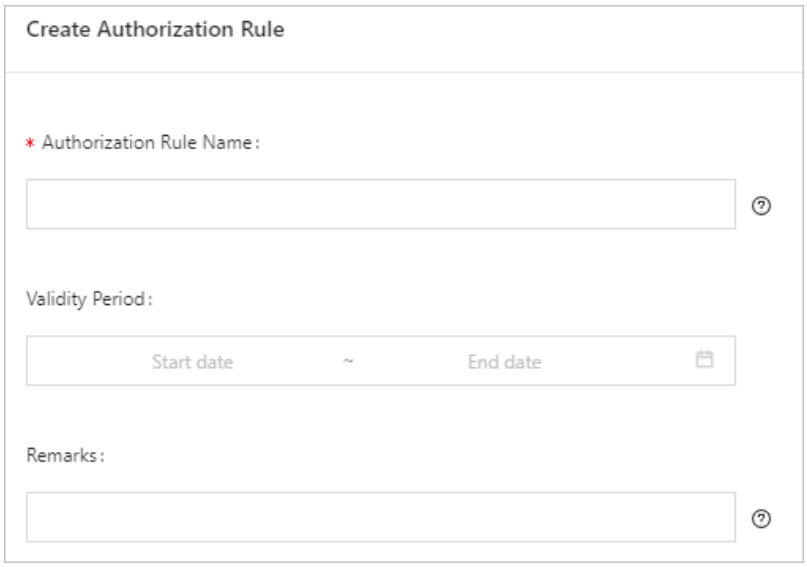
If the version of your Bastionhost is earlier than V3.2.22, you can authorize only a single user or user group to access hosts or host groups. You cannot specify the period of time in which the users can access the assets. If you want to create an authorization rule, you must update your Bastionhost to V3.2.22.

- For more information about the time ranges in which Bastionhost can be updated, see[Notice] Update Bastionhost to V3.2.22.
- For more information about how to update Bastionhost, see Update a bastion host.

Procedure

1.

2. In the left-side navigation pane, click **Authorization Rules**.
3. On the **Authorization Rules** page, click **Create Authorization Rule**.
4. In the **Create Authorization Rule** panel, configure the parameters such as **Authorization Rule Name** and **Validity Period**.



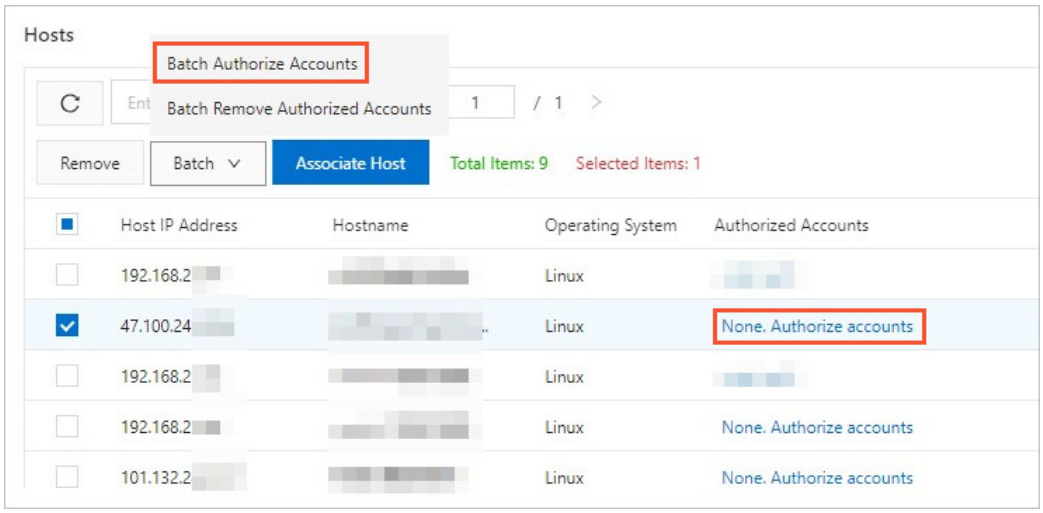
Parameter	Description
Authorization Rule Name	The name of the authorization rule.
Validity Period	The validity period of the authorization rule. You can specify the dates and points in time at which the validity period starts and ends based on your requirements.
Remarks	The remarks of the authorization rule.

5. Click **Create Authorization Rule**.
6. In the Create Authorization Rule panel, click **Associate with User**.
7. On the **Authorization Details** page, configure the hosts and users.

i. **Configure hosts or host groups**

- a. Click **Associate Host** or Associate Host Group.
  b. In the **Associated Host** or Associate Host Group panel, select the host or host group that you want to associate with the authorization rule.
  c. Click **OK**.
  d. Optional. If **None. Authorize accounts** is displayed in the **Authorized Accounts** column after you associate the hosts or host groups with the authorization rule, click **None. Authorize accounts** to authorize the accounts of the users to manage the hosts or host groups. You can select multiple hosts or host groups and authorize the accounts to manage the hosts or host groups at a time.

  You can also select multiple hosts or host groups to remove the authorized accounts at a time.



ii. **Configure users or user groups**

- a. Click **Associate User** or Associate User Group.
  b. In the **Associate User** or Associate User Group panel, select the user or user group that you want to associate with the authorization rule.
  c. Click **OK**.

After you complete the configuration, you can view the hosts, host groups, users, and user groups that you associate with the authorization rule in the Hosts, Host Groups, Users, and User Groups lists.

Result

After you create the authorization rule, the users and user groups that are associated with the authorization rule can access the selected hosts and host groups within the **Validity Period** that you specify for the authorization rule.

1.6.2. Manage an authorization rule

If you want to modify the configurations of an authorization rule or you no longer need to maintain an authorization rule that expires, you can modify or delete the authorization rule. This topic describes how to modify and delete an authorization rule.

Prerequisites

An authorization rule is created in your bastion host. For more information, see Create an authorization rule.

Modify an authorization rule

You can modify the parameters on the **Basic Info** and **Host / User** tabs of an authorization rule.

1.
2. In the left-side navigation pane, click **Authorization Rules**.
3. On the **Authorization Rules** page, find the authorization rule that you want to modify.
4. Click **Edit** in the Actions column.
5. On the Authorization Details page, modify the configurations of the authorization rule.
   - Modify the parameters on the **Basic Info** tab.
     a. Modify the **Authorization Rule Name**, **Validity Period**, and **Remarks** parameters.
     b. Click **Update**.
   - Modify the parameters on the **Host / User** tab.

     You can add or remove hosts and users for the authorization rule. You can adjust hosts, host groups, users, and user groups in the same manner.

     The following example shows how to adjust the hosts of an authorization rule.

     a. Click the **Host / User** tab.
     b. In the Hosts section, click **Associate Host** to add a host. You can also select the host that you want to remove and click **Remove** to remove the host.

   After you modify the authorization rule, your bastion host runs based on the modified authorization rule.

Delete an authorization rule

If you no longer need an authorization rule, you can delete the authorization rule.

1.
2. In the left-side navigation pane, click **Authorization Rules**.
3. On the **Authorization Rules** page, find the authorization rule that you want to delete.
4. Click **Delete** in the Actions column.
5. In the message that appears, click **Delete**.
   After you delete the authorization rule, the configurations such as the assets that are associated with the rule and the validity period of the rule become invalid.

1.7. policies

1.7.1. Create a control policy

Bastionhost provides the control policy feature. You can use this feature to configure command control, command approval, protocol control, and access control policies to manage the access of users to hosts. This topic describes how to create a control policy.

Procedure

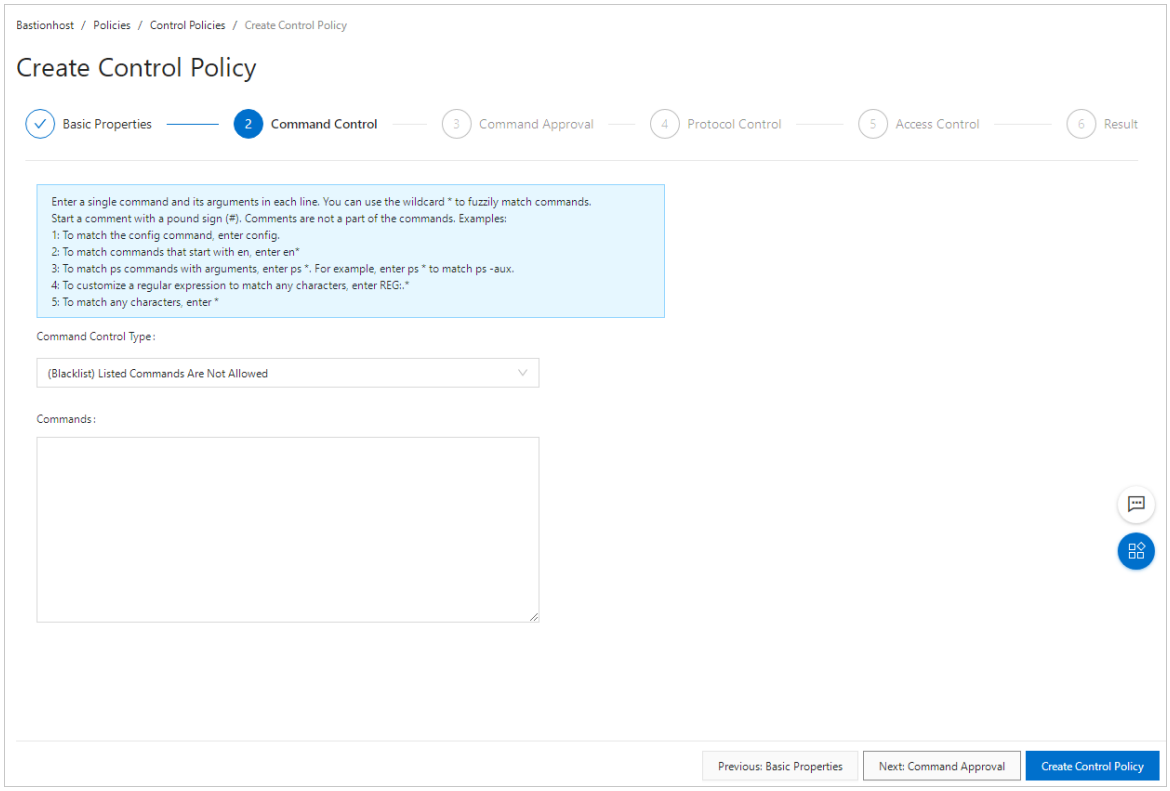
1.
2.
3.
4. In the Basic Properties step of the Create Control Policy wizard, configure **Name**, **Priority**, and **Remarks**. Then, click **Next: Command Control (Optional)**.

   > **Note**
   > - You can set the Priority parameter to a value that ranges from 1 to 100. The default value is 1, which indicates the highest priority.
   > - You can configure the same priority for different control policies. If multiple control policies have the same priority, Bastionhost determines the order in which the policies take effect based on specific rules defined in these policies. Command-related rules are prioritized in descending order: reject, allow, and approve. In access control policies, a blacklist has a higher priority than a whitelist.

5. In the Command Control step, configure **Command Control Type** and **Commands**. Then, click **Next: Command Approval (Optional)**.

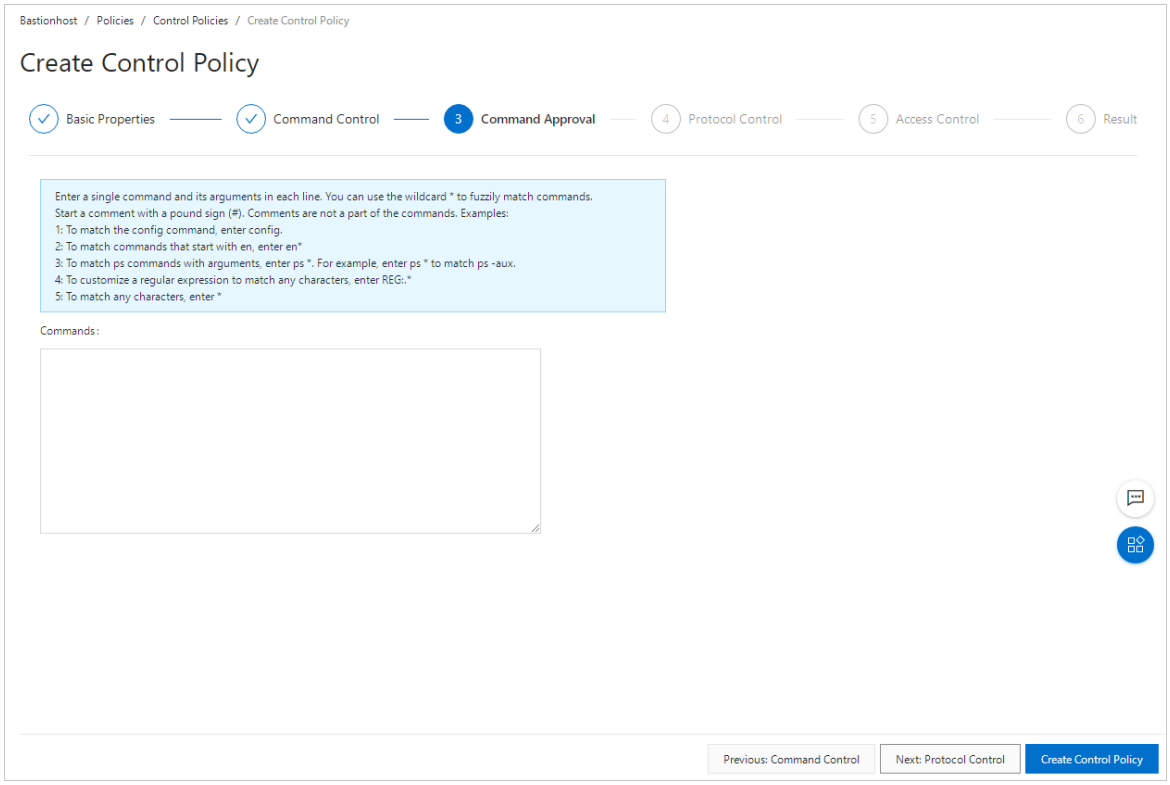
   You can select **(Whitelist) Only Listed Commands Are Allowed** or **(Blacklist) Listed Commands Are Not Allowed** for the Command Control Type parameter.

   - **(Whitelist) Only Listed Commands Are Allowed**: If you select this option, the Commands field is required. Only the commands in a whitelist can be run by the users and on the hosts to which the policy applies.
   - **(Blacklist) Listed Commands Are Not Allowed**: If you select this option, the Commands field can be left empty. The commands in a blacklist cannot be run by the users and on the hosts to which the policy applies.



6. In the Command Approval step, configure **Commands** and click **Next: Protocol Control (Optional)**.

   A command approval policy is used to approve the commands that are not included in the whitelist or blacklist of a command control policy. The command control policy takes precedence over the command approval policy in validation. If users run the commands specified by the Commands field in the Command Approval step, you can choose whether to approve the execution of the commands in the Bastionhost console. Only the commands that pass the approval can be run. For more information, see Approve commands.



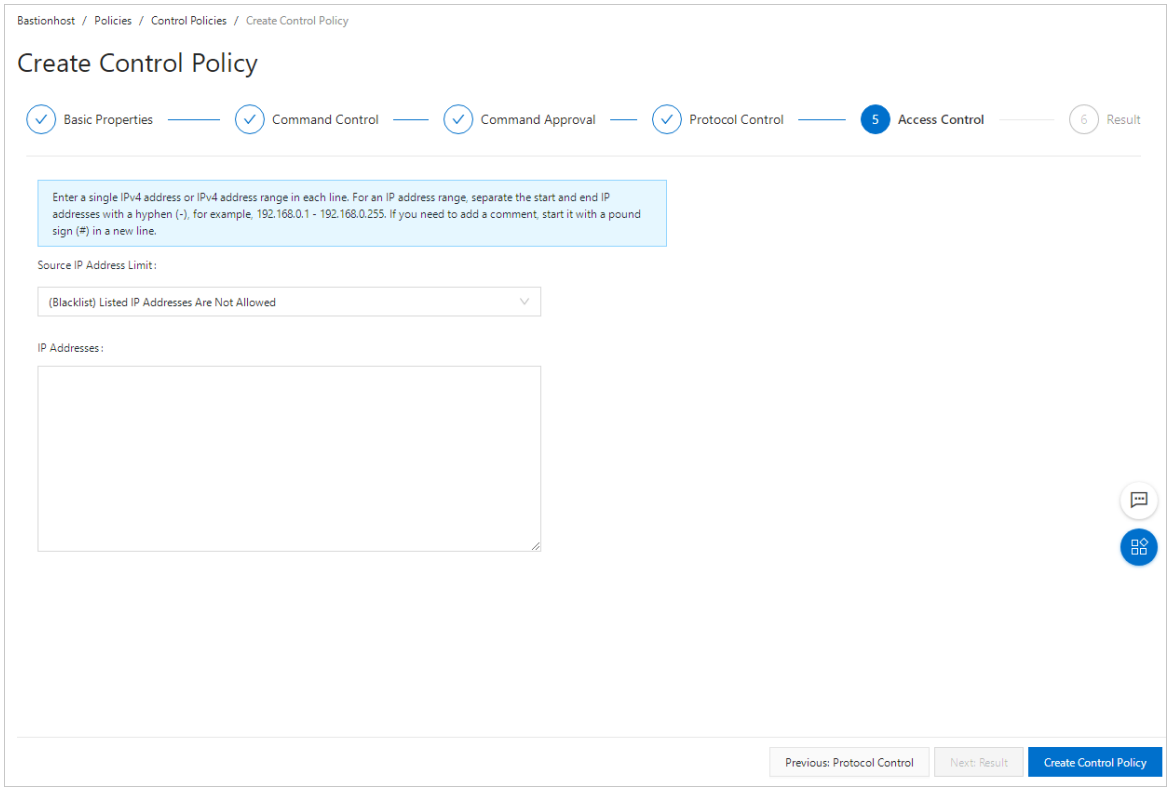
7. In the Protocol Control (Optional) step, configure **RDP Options**, **SSH Options**, and **SFTP Options**. Then, click **Next: Access Control (Optional)**.

   After you select required options, the users to which the policy applies can perform corresponding operations. If you select File Upload, the users can upload files.

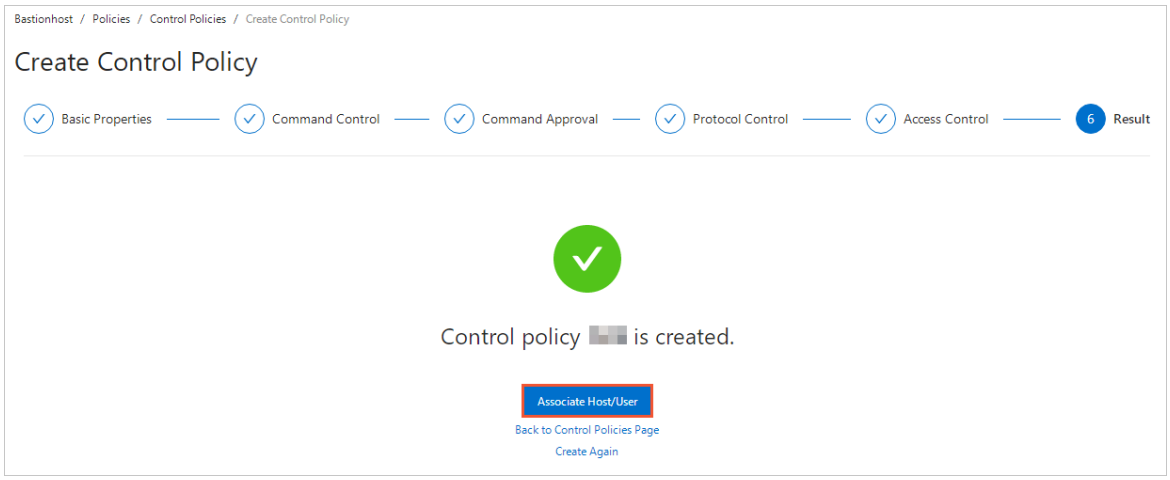
8. In the Access Control (Optional) step, configure Source IP Address Limit and IP Addresses and click **Create Control Policy**.

   You can select one of the following options for the Source IP Address Limit parameter:

   - **(Whitelist) Only Listed IP Addresses Are Allowed**: If you select this option, the IP Addresses field is required. Users can use only the source IP addresses in a whitelist to access the hosts to which the policy applies.
   - **(Blacklist) Listed IP Addresses Are Not Allowed**: If you select this option, the IP Addresses field can be left empty. Users cannot use the source IP addresses in a blacklist to access the hosts to which the policy applies.



9. (Optional)In the Result step, click **Associate Host/User**.



You can associate the policy with one or more users or hosts for the policy to take effect on these users or hosts. For more information, see Associate hosts or users.

1.7.2. Manage control policies

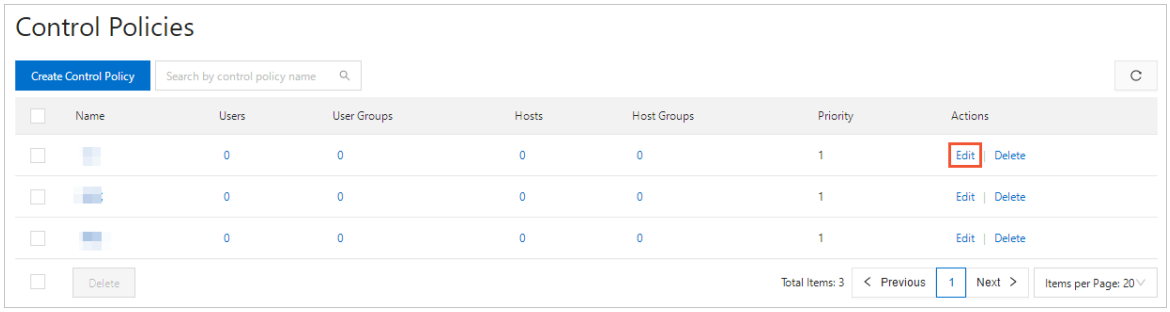
This topic describes how to modify or delete existing control policies to meet your business requirements. This topic also describes how to associate a control policy with hosts and users.

Modify a control policy

To modify an existing control policy, perform the following steps:

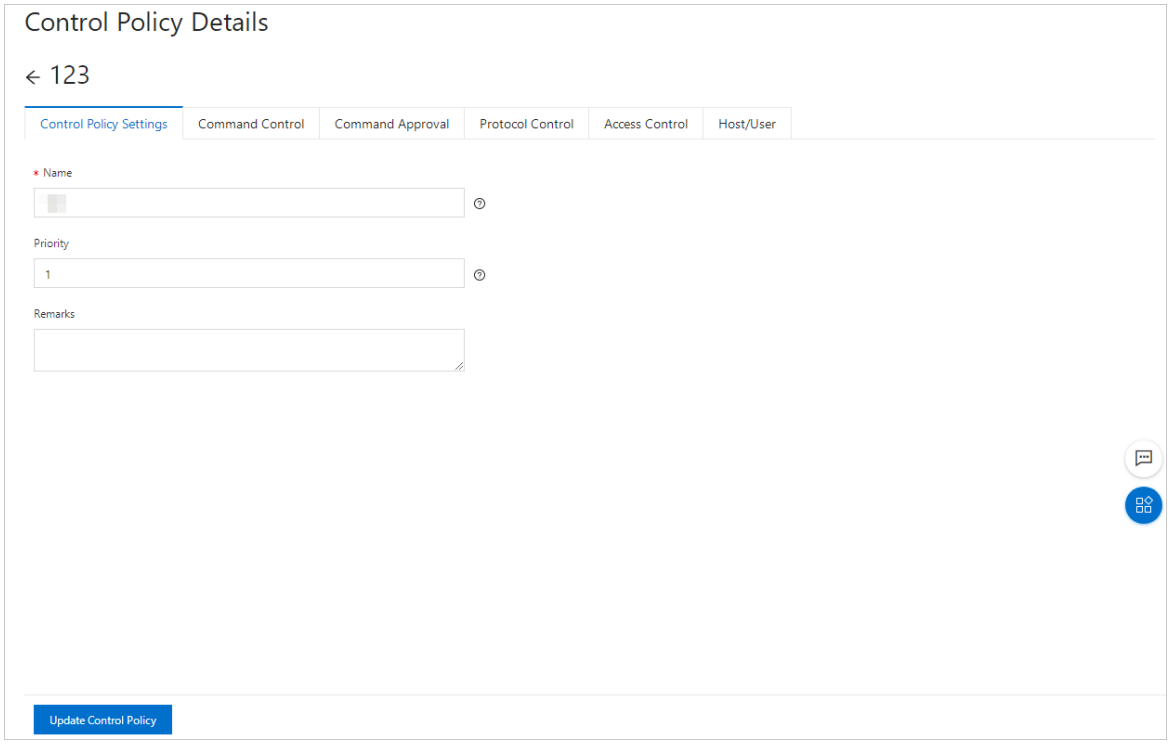
1.
2.

3. In the control policy list, find the control policy that you want to modify and click **Edit** in the **Actions** column.



Alternatively, you can click the name of the control policy that you want to modify to go to the **Control Policy Details** page.

4. On the **Control Policy Details** page, modify settings on the following tabs: **Control Policy Settings**, **Command Control**, **Command Approval**, **Protocol Control**, **Access Control**, and **Host/User**.



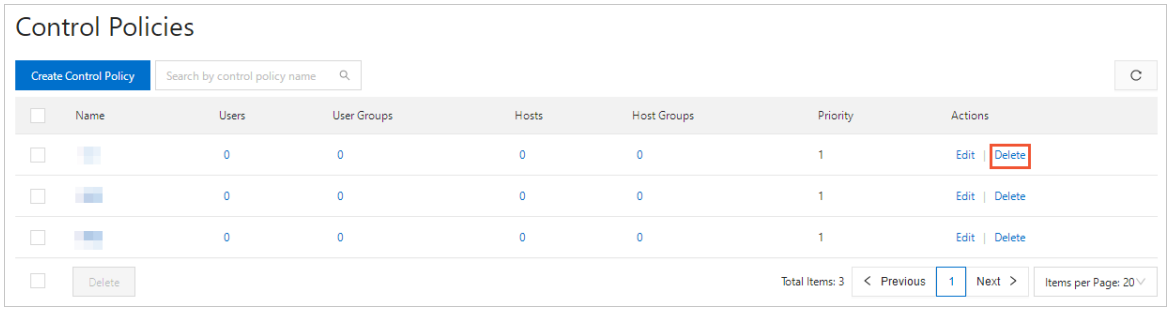
For more information about how to modify settings on the **Control Policy Settings**, **Command Control**, **Command Approval**, **Protocol Control**, and **Access Control** tabs, see Create a control policy. For more information about how to associate a control policy with hosts or users on the **Host/User** tab, see Associate hosts or users.

5. Click **Update Control Policy** in the lower-left corner.

Delete a control policy

To delete a control policy that you no longer use, perform the following steps:

1.
2.
3. Find the control policy that you want to delete and click **Delete** in the Actions column.



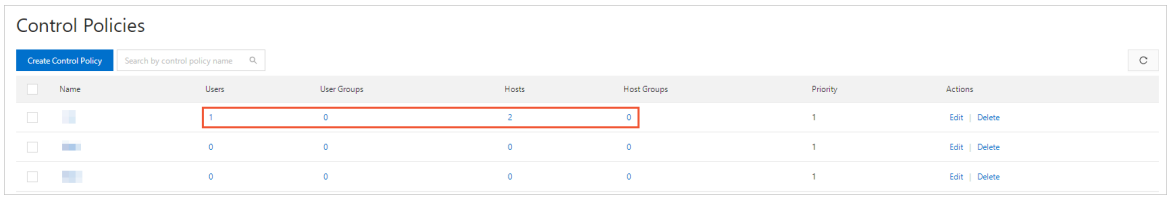
To delete multiple control policies at a time, select the control policies and click **Delete** in the lower-left corner.

4. In the message that appears, click **Delete**.

Associate hosts or users

To associate a control policy with users or hosts or modify the existing association of a control policy, perform the following steps:

1.
2.
3. Find a control policy and click the number in the **Users**, **User Groups**, **Hosts**, or **Host Groups** column.



Alternatively, you can click the name of the control policy or click **Edit** in the Actions column, and click the **Host / User** tab.

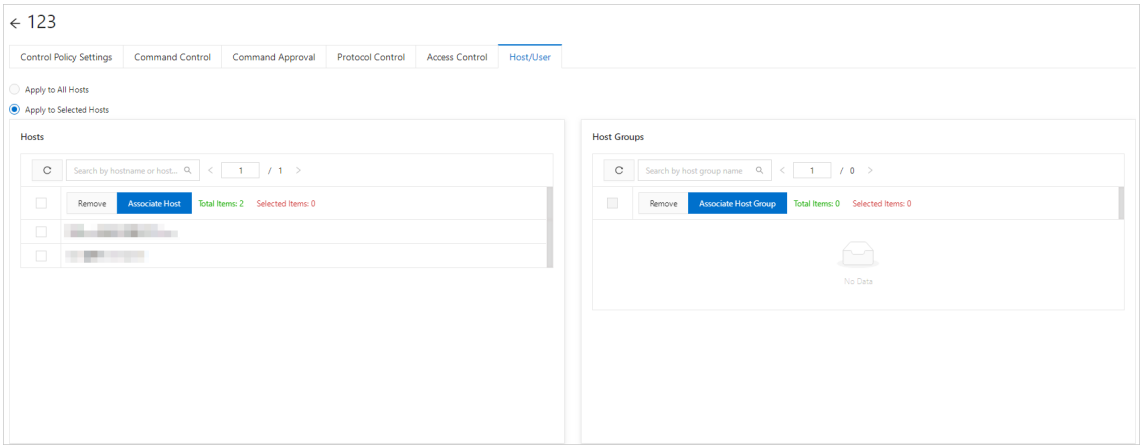
4. Select the validation mode for the control policy.

> **Note** The selected validation mode for a control policy immediately takes effect. We recommend that you confirm the policy validation mode before you proceed with relevant operations.

You can select a policy validation mode based on the following information:

- Select a policy validation mode for hosts.

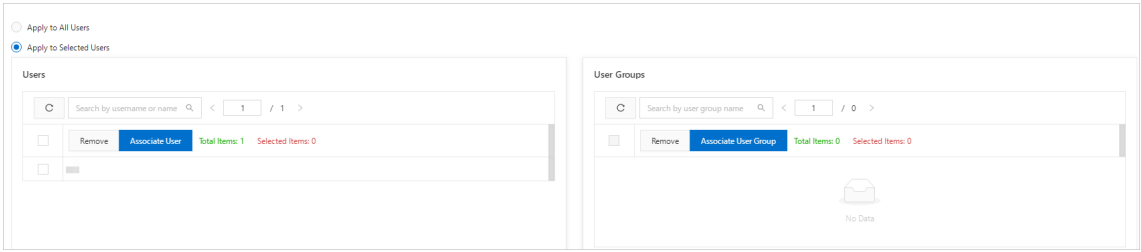
  You can select **Apply to All Hosts** or **Apply to Selected Hosts**. If you select **Apply to Selected Hosts**, you must select the hosts or host groups with which you want to associate the control policy. The control policy applies only to the associated hosts or host groups.



> **Note** If multiple control policies with the same priority are validated on the same host at the same time, Bastionhost determines the validation order of the policies based on specific rules defined in these policies. Command-related rules are prioritized in descending order: reject, allow, and approve. In access control policies, a blacklist has a higher priority than a whitelist.

- Select a policy validation mode for users.

  You can select **Apply to All Users** or **Apply to Selected Users**. If you select **Apply to Selected Users**, you must select the users or user groups with which you want to associate the control policy. The control policy applies only to the associated users or user groups.



If some hosts or users no longer need the control policy, you can select these hosts or users and click **Remove** to remove them from the policy validation list.

1.8. Approval

1.8.1. Approve commands

When a user runs commands that are configured to be approved in the control policy associated with the user on a host (associated with this control policy), you receive a notification to approve the commands as an administrator. The commands are executed only after you approve them as an administrator. The commands in the command control list do not require approval. This topic describes how to approve commands as an administrator.

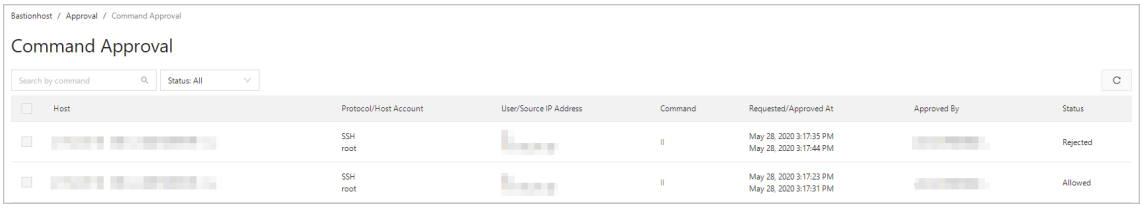
Procedure

1.
2.
3. On the **Command Approval** page that appears, perform the following operations as needed:

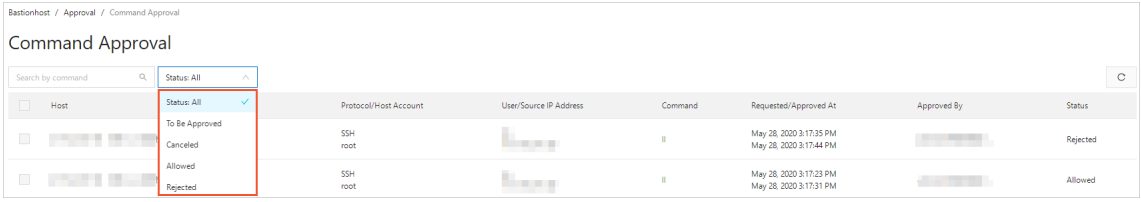
   - **View command details**

- View command details

  You can view the settings of the following parameters of the listed commands: **Host**, **Protocol/Host Account**, **User/Source IP Address**, **Command**, **Requested/Approved At**, **Approved By**, and **Status**.

  You can select a state from the status drop-down list in the upper-left corner to view all the commands that are in this state. For example, if you select **To Be Approved**, you can view all the commands that are in this state.

  The following states are supported:

  - **All**: the commands in all states
  - **To Be Approved**: the commands to be approved
  - **Canceled**: the commands of which the execution is canceled
  - **Allowed**: the commands that are allowed to be executed
  - **Rejected**: the commands that are disallowed to be executed

- **Allow command execution**

  Select the target commands and click **Allow** in the lower-left corner of the command approval list.

- **Reject command execution**

  Select the target commands and click **Reject** in the lower-left corner of the command approval list.

1.9. Auditing

1.9.1. Session audit

1.9.1.1. Search for sessions and view session details

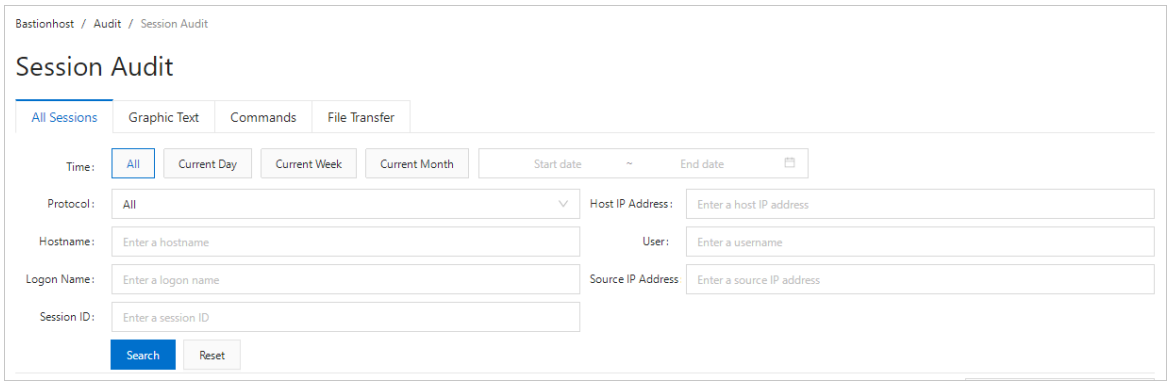
Each time an O&M operation is performed in Bastionhost, a session is generated to record the O&M operation. Auditors can audit the session to check whether an unauthorized operation is performed.

Prerequisites

Flash Player that is used to play session videos is installed in your browser.

Search for sessions

1.
2.
3. On the Session Audit page, click the **All Sessions**, **Graphic Text**, **Commands**, or **File Transfer** tab.



The following list describes the sessions that you can query on the **Graphic Text**, **Commands**, and **File Transfer** tabs.

- **Graphic Text**: You can query the sessions of O&M operations that are performed on servers by using your bastion host in RDP mode. You can query the sessions of O&M operations only on servers that run Windows Server 2008 or earlier versions.
- **Commands**: You can query the commands that are used to perform O&M operations on servers by using your bastion host in SSH mode.
- **File Transfer**: You can query the sessions of O&M operations, such as file upload, file deletion, and file renaming, that are performed on servers by using your bastion host.

4. Configure search conditions.

The following table describes the search conditions that you can configure.

Search condition	Description
Time	Specify the search time range. Valid values: **All**, **Current Day**, **Current Week**, and **Current Month**. You can also specify a custom time range.
Protocol	Select a protocol type from the Protocol drop-down list. Valid values: **All**, **SSH**, **SFTP**, and **RDP**.
Host IP Address	Enter the IP address of the host in the session that you want to view.
Hostname	Enter the name of the host in the session that you want to view.
User	Enter the name of the user whose session you want to view.
Logon Name	Enter the name of the account that is used by the user to log on to the host.
Source IP Address	Enter the IP address that is used by the user to perform O&M operations.
Session ID	Enter the session ID.

Search condition	Description
Deletion Status	Select a session deletion state. Valid values: ○ **All** ○ **Undeleted** ○ **Deleted**

5. (Optional)Click **Save**. In the Save dialog box, specify **Filter Template** and click **OK** to save the search conditions.

   > **Note** After you save the search conditions as a template, you can use the same conditions again when you select the template name from the **Default Condition** drop-down list in the upper-right corner of the list of session search results.

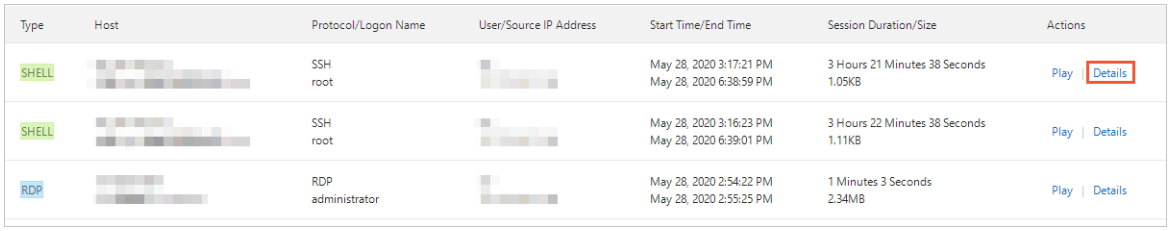
6. Click **Search**.

View session details

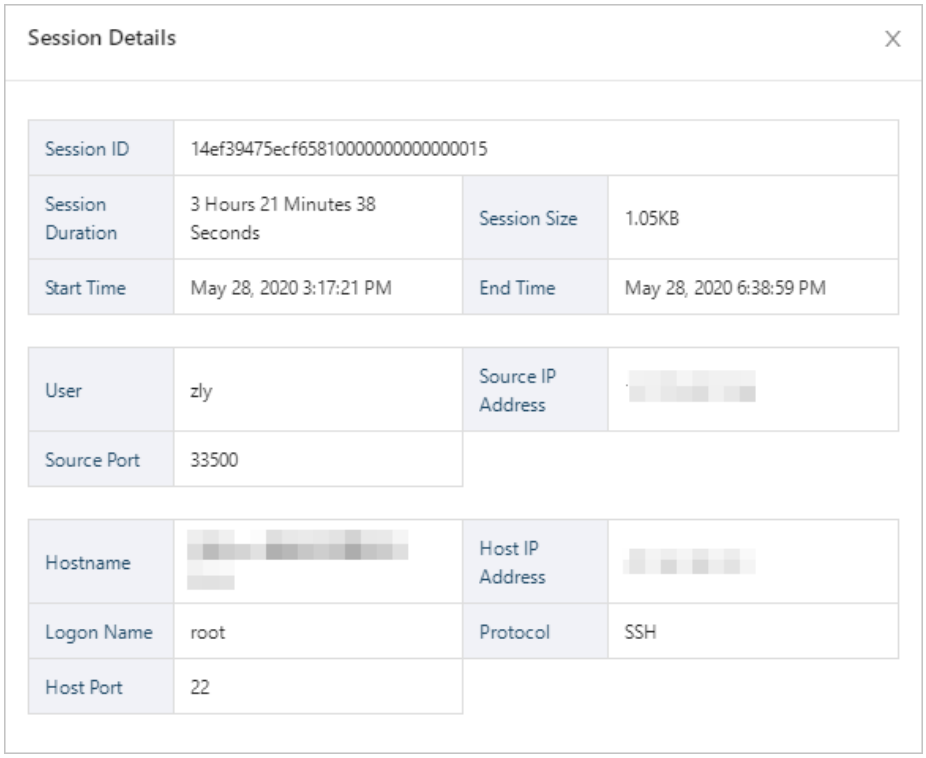
1. Search for a session.

   For more information, see Search for sessions.

2. Find the session and click **Details** in the **Actions** column.



3. In the **Session Details** panel, view the basic information about the session, user, and host.

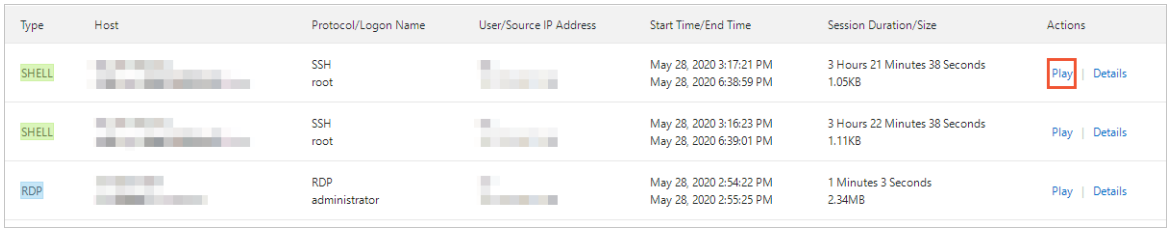


Play session videos

1. Search for a session.

   For more information, see Search for sessions.

2. Find the session and click **Play** in the **Actions** column.



1.9.1.2. Archive audit logs in Log Service

Bastionhost allows you to archive audit logs in Log Service. The audit logs record all O&M activities. After you configure the archiving settings for audit logs, Bastionhost automatically delivers the audit logs to Log Service. This topic describes how to archive audit logs in Log Service.

Context

Audit logs record the O&M activities that O&M engineers perform by using Bastionhost. Bastionhost stores audit logs only for 180 days. If you want to store audit logs longer than 180 days, you can archive the audit logs in Log Service. In the Log Service console, you can customize the log retention period. In addition, you can query and analyze the audit logs. For more information, see Log search overview and Log analysis overview.

> **Note** The archiving operation does not affect the audit logs that are stored in Bastionhost. You can still view these audit logs on the **Session Audit** page of the Bastionhost console. For more information, see Search for sessions and view session details.

Procedure

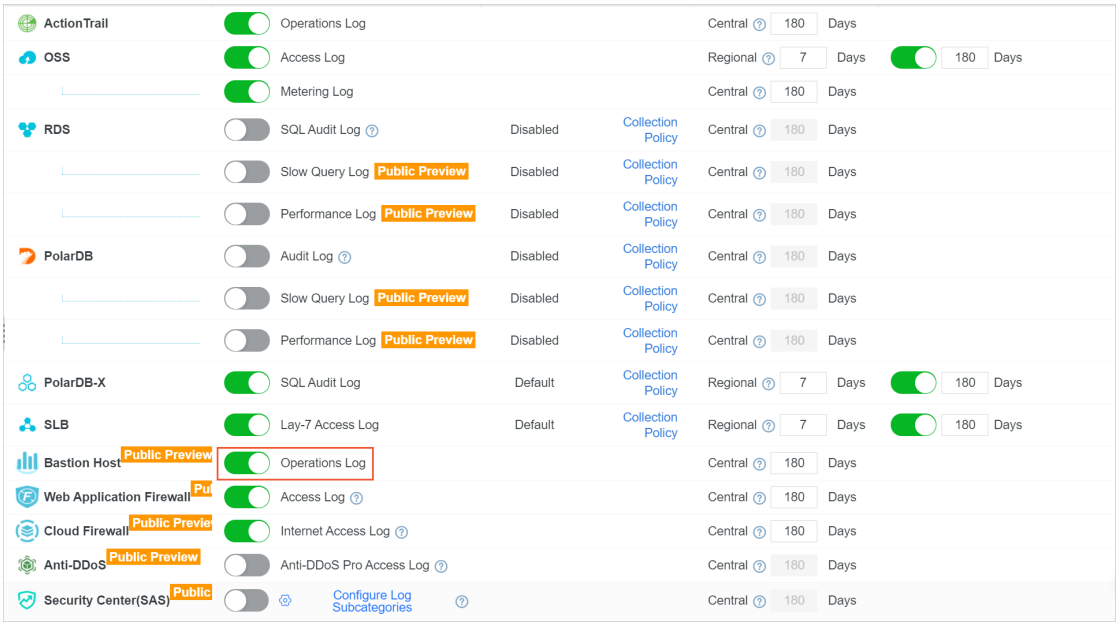
1. Log on to the Log Service console.
2. Activate Log Service as required.
3. In the **Log Application** section, click **Log Audit Service**.
4. On the **Global Configurations** tab, complete the settings for collecting audit logs.
   i. In the **Region of the Central Project** drop-down list, select the region of the project in which you want to centrally store the collected logs.
   ii. Authorize Log Service to collect and synchronize logs.

   You can select manual authorization or AccessKey pair-based authorization.

   - **AccessKey Pair-Based Authorization**: Enter the AccessKey ID and AccessKey secret of an authorized RAM user.

     The AccessKey ID and AccessKey secret are only for temporary use. The RAM user must be attached the AliyunRAMFullAccess policy.
   - **Manual Authorization**: For more information, see Use a custom policy to authorize Log Service to collect and synchronize logs.

   iii. Find Bastion Host in the Cloud Products column, turn on **Operations Log**, and then specify a retention period for audit logs in the **Storage Type** column.



5. View audit logs.
   i. On the left-side navigation sidebar, click the icon.
   ii. In the left-side navigation pane, click **Bastionhost** under **Central**.

iii. View the audit logs on the **Bastion Host** tab.

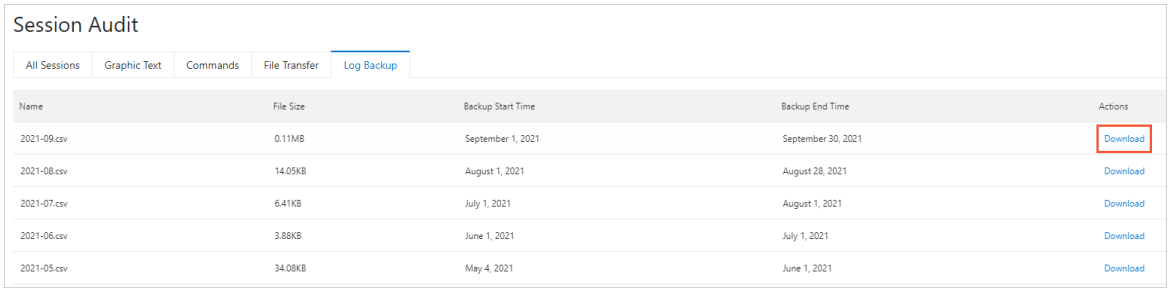
For more information about the fields of operation logs in Bastionhost, see Bastionhost.

1.9.1.3. Use the log backup feature

Bastionhost provides the log backup feature to help you better manage O&M logs. This feature backs up O&M logs and generates a log file that contains the logs once a month. You can download log files based on your business requirements. This topic describes how to use this feature.

Procedure

1.
2. In the left-side navigation pane, choose **Audit > Session Audit**.
3. On the **Session Audit** page, click the **Log Backup** tab.
4. On the **Log Backup** tab, find the log file that you want to download and click **Download** in the Actions column.
   The O&M logs are downloaded to your computer in the CSV format.



1.9.2. Real-time monitoring

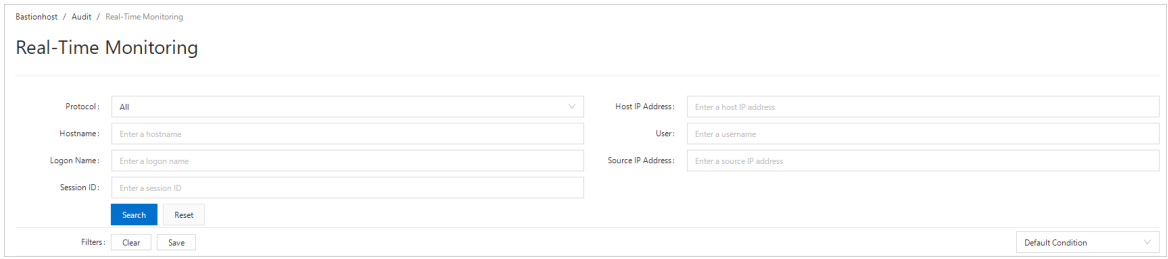
1.9.2.1. Search for real-time monitoring sessions and view session details

Each time users perform O&M operations in Bastionhost, a session is generated to record the O&M operations. Auditors can monitor the session in real time to check whether an unauthorized operation is performed.

Prerequisites

Search for sessions

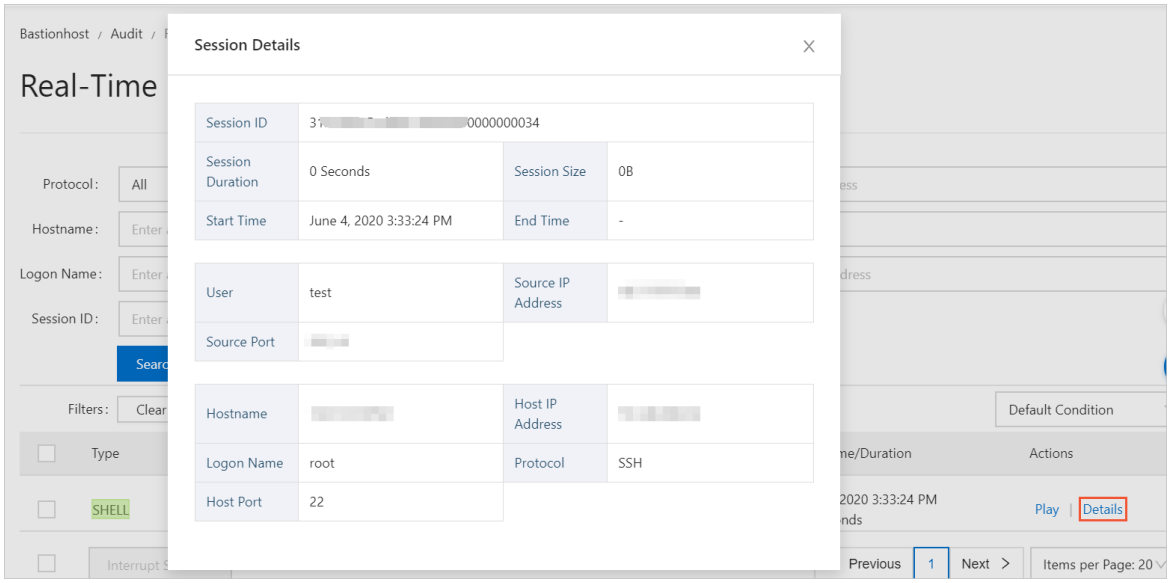
1.
2.
3. On the Real-Time Monitoring page, configure search conditions.



4.
5.

View session details

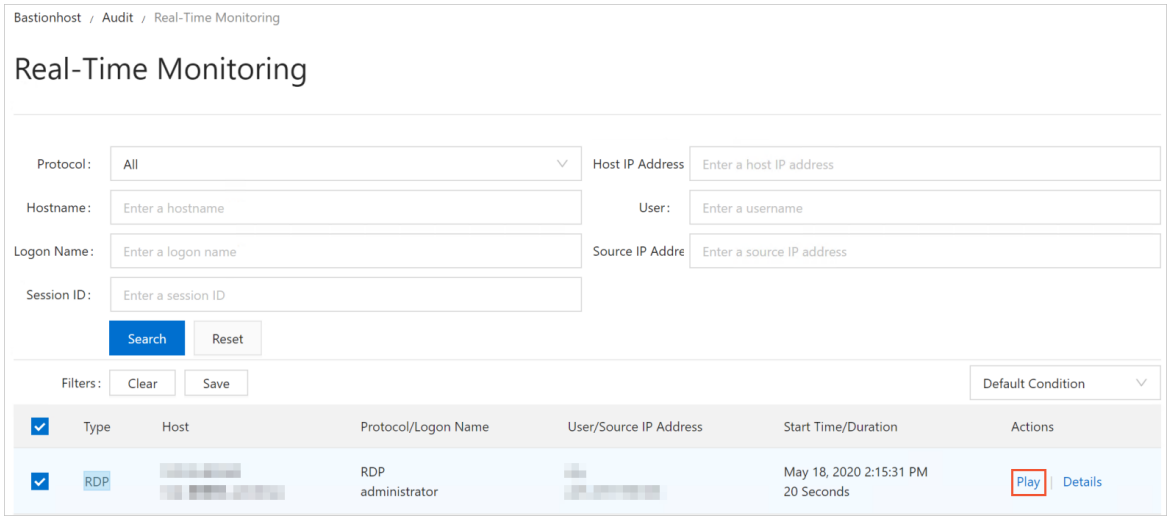
1.
2.
3. On the Real-Time Monitoring page, find the session whose details you want to view and click **Details** in the **Actions** column.



In the **Session Details** panel, you can view basic information about the session, user, and host.

Play session videos

1.
2.
3. Find the session video that you want to play and click **Play** in the **Actions** column.



1.9.2.2. Interrupt sessions

If you notice that a user is performing an unauthorized or high-risk operation on a host during real-time monitoring, you can use the session interruption feature to disconnect the user from the host.

Interrupt sessions on the Real-Time Monitoring page

1.
2.
3. On the Real-Time Monitoring page that appears, select one or more sessions that you want to interrupt.

4. Click **Interrupt Sessions** in the lower-left corner of the session search result list.

1.9.3. Operations logs

1.9.3.1. Search for operation logs and view log details

All operations performed in Bastionhost are recorded in operation logs. This topic describes how to search for operation logs and view log details on the Operations Logs page.

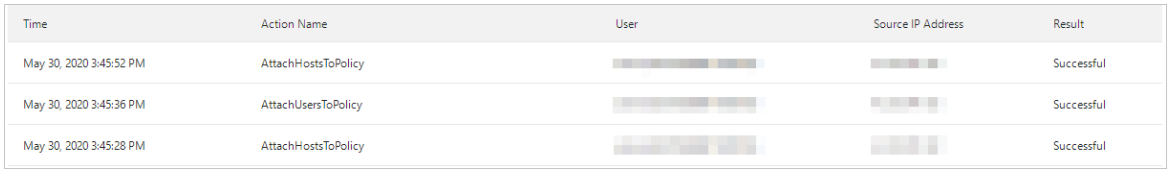
Procedure

1.
2.
3. Configure search conditions.

Time	Specify the search time range. Valid values: **All**, **Current Day**, **Current Week**, and **Current Month**. You can also specify a custom time range.

Result	Select the result of the operation that you want to view from the Result drop-down list. Valid values: ○ **All** ○ **Successful** ○ **Failed**
Action Name	Select the operation that you want to view from the Action Name drop-down list.
	Enter the name of the user whose operation logs you want to view.
	Enter the IP address used by the user to perform O&M operations.

4.
5. Click **Search**.
6. View the log details that meet the search conditions in the log search result list.



Time	Action Name	User	Source IP Address	Result
May 30, 2020 3:45:52 PM	AttachHostsToPolicy			Successful
May 30, 2020 3:45:36 PM	AttachUsersToPolicy			Successful
May 30, 2020 3:45:28 PM	AttachHostsToPolicy			Successful

1.9.4. O&M reports

The administrator of Bastionhost can view O&M reports, including the overall O&M data, size of O&M session data, number of O&M sessions, and O&M duration. The administrator can specify the time range to view the reports. This topic describes the details of O&M reports.

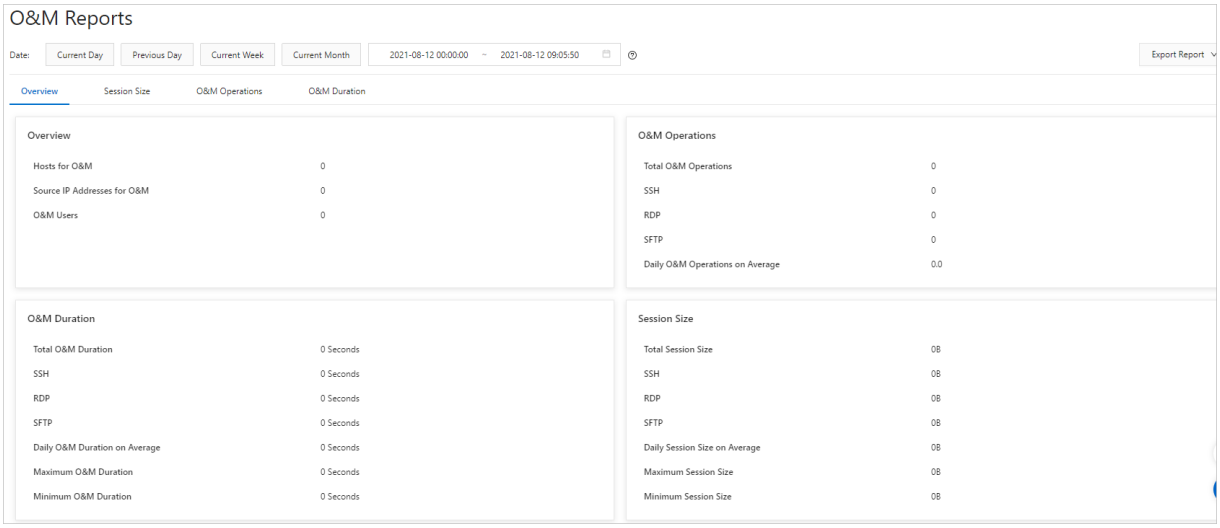
Description

You can click **Current Day**, **Previous Day**, **Current Week**, or **Current Month** to view O&M data. You can also specify a time range to view O&M data. The following table describes the time ranges.

Time range	Description
Current Day	The time ranges from 00:00:00 of the current day to the current point in time.
Previous Day	The time ranges from 00:00:00 to 24:00:00 on the last day.
Current Week	The time ranges from 00:00:00 on Monday of the current week to the current point in time.
Current Month	The time ranges from 00:00:00 on the first day of the current month to the current point in time.
Custom time range	The time range is customized and can span up to 180 days.

Overview

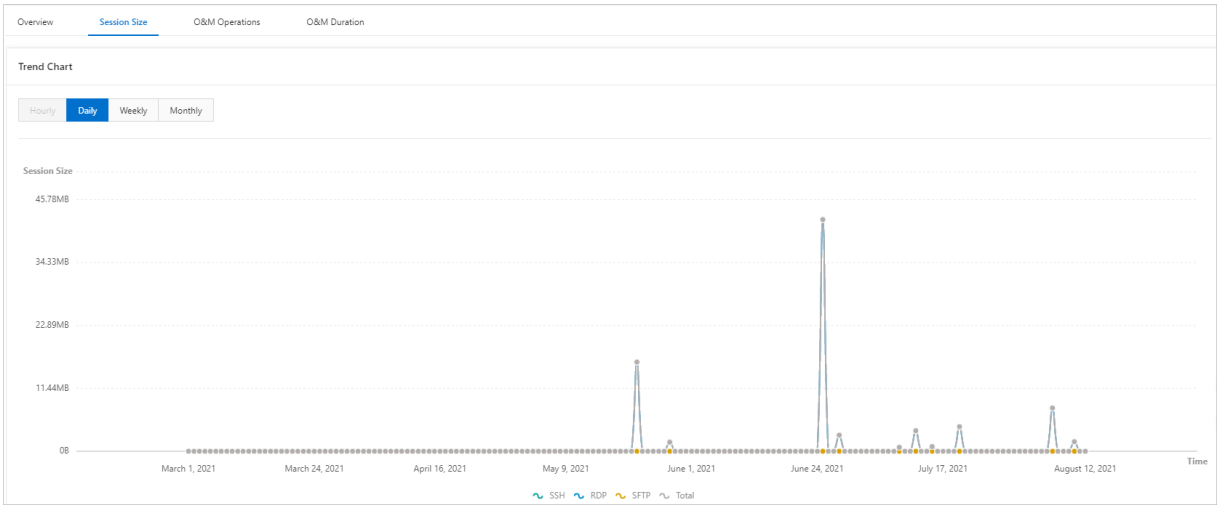
The Overview tab displays the O&M data within the specified time range on the **Overview**, **O&M Operations**, **O&M Duration**, and **Session Size** tabs.



Session Size

The Session Size tab displays the trend on the size of O&M session data within the specified time range in the **Trend Chart** section and the session details in the **Details** section. In the **Trend Chart** section, you can click **Hourly**, **Daily**, **Weekly**, or **Monthly** to view the size of session data within a more precise time range.

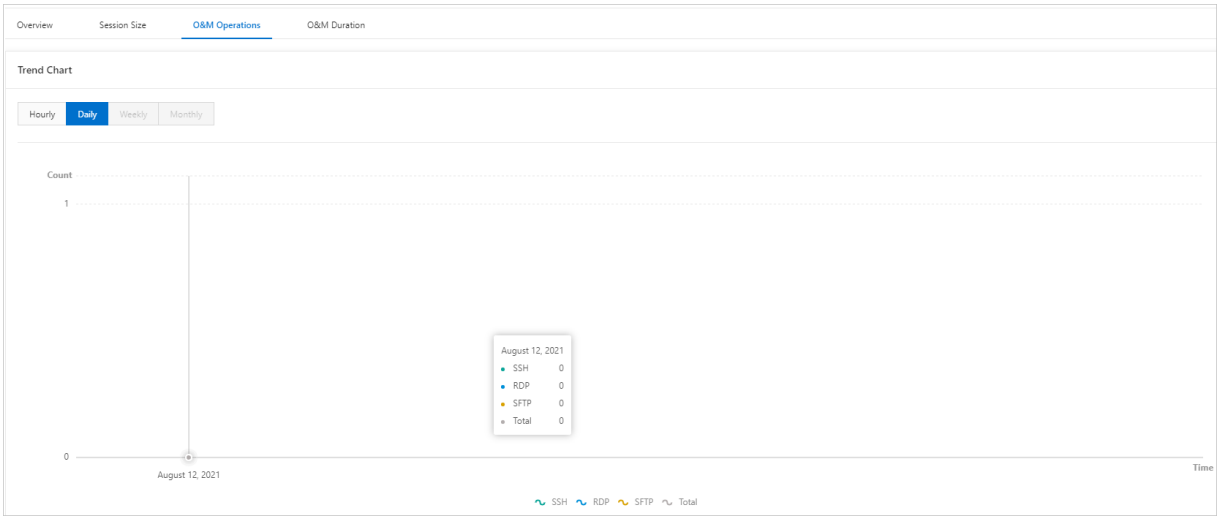
- **Trend Chart**: the trend on the size of O&M session data within the specified time range.
- **Details**: the sizes of session data within the specified time range. The sizes are displayed from the **SSH**, **RDP**, **SFTP**, and **Total** dimensions.



O&M Operations

The O&M Operations tab displays the trend on the number of O&M sessions within the specified time range in the **Trend Chart** section and the details about the O&M sessions in the **Details** section. In the **Trend Chart** section, you can click **Hourly**, **Daily**, **Weekly**, or **Monthly** to view the number of O&M sessions within a more precise time range.

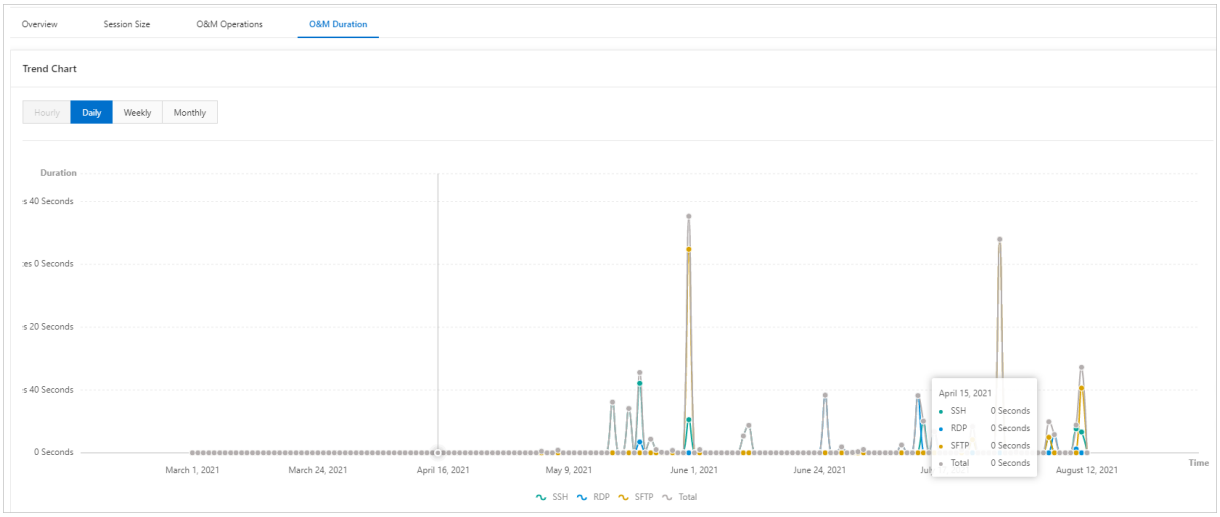
- **Trend Chart**: the trend on the number of O&M sessions in the specified time range.
- **Details**: the numbers of O&M sessions within the specified time range. The numbers are displayed from the **SSH**, **RDP**, **SFTP**, and **Total** dimensions.



O&M Duration

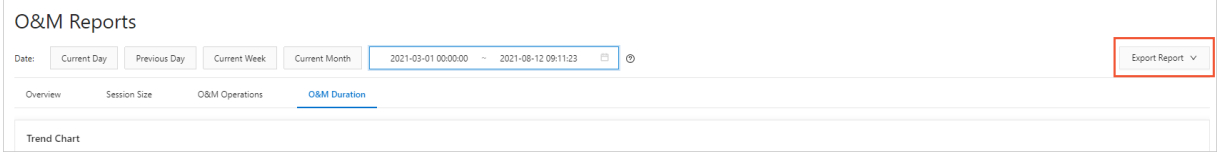
The O&M Duration tab displays the trend of O&M durations within the specified time range in the **Trend Chart** section and the details about the O&M durations in the **Details** section. In the **Trend Chart** section, you can click **Hourly**, **Daily**, **Weekly**, or **Monthly** to view the O&M durations within a more precise time range.

- **Trend Chart**: the trend of the O&M duration within the specified time range.
- **Details**: the O&M durations within the specified time range. The durations are displayed from the **SSH**, **RDP**, **SFTP**, and **Total** dimensions.



Export Report

In the upper-right corner of the O&M Reports page, you can click **Export Report** to export the O&M reports within the specified time range. The O&M reports can be saved as Word, PDF, or HTML files.



1.10. O&M

1.10.1. Use the host O&M feature

After a regular user logs on to the Bastionhost console as a Resource Access Management (RAM) user, the user can go to a web page to perform O&M operations on hosts. The user does not need to use an SSH, Remote Desktop Protocol (RDP), or SSH File Transfer Protocol (SFTP) client. This topic describes how to use the host O&M feature.

Limits

- Only Bastionhost HA Edition supports the host O&M feature.
- You can use the host O&M feature only after you log on to the Bastionhost console as a RAM user.

Preparations

1. Create a RAM user and import the user. For more information, see Manage users.

   > **Note** If you have created a RAM user, import the created RAM user. For more information, see Import a created RAM user.

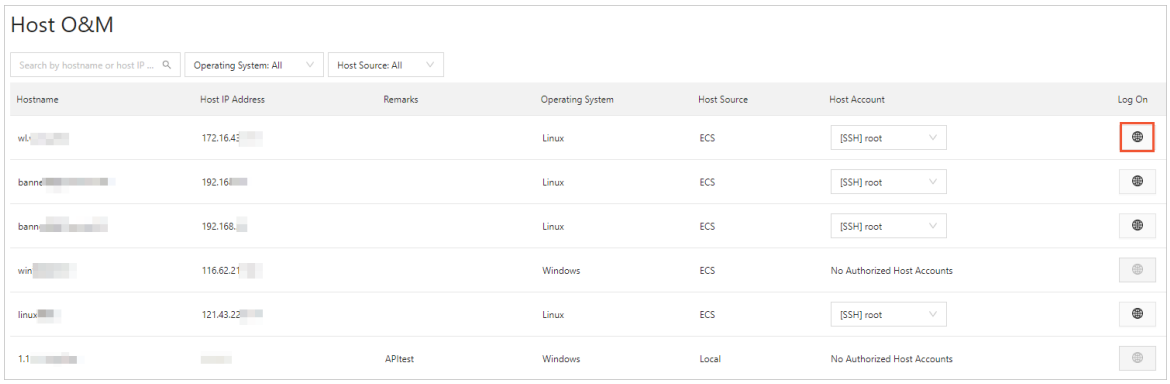
2. Add a host. For more information, see Add hosts.

   > **Note** If you want to manage host accounts in Bastionhost, you can create an account for a host. For more information, see Create an account for a host.

3. Authorize the host for the RAM user. For more information, see Authorize a user to manage hosts and Authorize a user to manage host groups.

Procedure

1. Log on to the Bastionhost console.
2. In the left-side navigation pane, choose **O&M > Host O&M**.
3. On the **Host O&M** page, find the host on which you want to perform O&M operations and click the icon in the Log On column. The host O&M page appears.



If the host is not authorized, the **O&M Logon** dialog box appears after you click the icon.

i. In the **O&M Logon** dialog box, specify the **Logon Name** and **Password** parameters.
   - **Logon Name**: the name of the account that is used to log on to the host.
   - **Password**: the password of the account that is used to log on to the host.

   > **Note** By default, the Protocol parameter is specified. You do not need to specify this parameter.

ii. Click **OK**.

4. Go to the O&M web page of the host and perform O&M operations on the host.

1.11. System settings

1.11.1. Configure the parameters on the User Settings tab

To ensure system security, you can configure account lockout policies and mark accounts that are inactive for a long period of time. You can configure account lockout policies to protect your resources against brute-force attacks. You can also configure the parameters in the User Status Settings section to specify the validity period of passwords and mark accounts that are inactive for a long period of time.

Procedure

1.
2.
3. On the **User Settings** tab, configure the following parameters.

Parameter		
	Account Lockout Threshold	The number of consecutive failed logon attempts that cause an account to be locked. Valid values: 0 to 999. Default value: 5. If you set this parameter to **0**, the system never locks an account.
	Account Lockout Duration	The duration within which a locked account cannot be used to log on to the system. Unit: minutes. Valid values: 0 to 10080. Default value: 30. If you set this parameter to **0**, an account is locked until the administrator unlocks the account.

Parameter		
Account Lockout Policy		
	Reset Account Lockout Counter After	The period of time that must elapse from the time a user fails to log on to the system before the failed logon attempt counter is reset to 0. This parameter takes effect when the number of failed logon attempts does not exceed the specified value of **Account Lockout Threshold**. Unit: minutes. For example, you set **Account Lockout Threshold** to **5** and **Reset Account Lockout Counter After** to **5**. If you use an invalid password to attempt to log on to the system for the fourth time at 14:00:00 and you do not use an invalid password to attempt to log on to the system again from 14:00:00 to 14:05:00, the failed logon attempt counter is reset to 0 after 14:05:00 on the current day. Valid values: 0 to 10080. Default value: 5.
User Status Settings	**Password Validity Period**	The validity period of a password. After the validity period elapses, password reset is required. This parameter takes effect only for local users. Valid values: 0 to 365. Default value: 0. Unit: days. If you set this parameter to **0**, a password never expires.
	Inactive User Account	The number of days after which an account is marked as Inactive. If an account is not used to log on to the system within the specified period of time, the account is marked as Inactive. Unit: days. Valid values: 0 to 365. Default value: 0. If you set this parameter to **0**, an account is never marked as Inactive.
	Automatic Synchronization of Status of AD-authenticated Or LDAP-authenticated Users	The interval at which the configurations and status of the Active Directory (AD)-authenticated or Lightweight Directory Access Protocol (LDAP)-authenticated users imported into Bastionhost are automatically synchronized. Unit: minutes. Valid values: 15 to 14400. Default value: 240.

4. Click **Save**.

1.11.2. Enable two-factor authentication

After a user logs on to the Bastionhost console by using the username-password logon method, you can enable two-factor authentication to allow the user to enter a dynamic verification code that is sent by using a text message, an email, or a notification in DingTalk. This reduces the risk of password leaks. This topic describes how to enable two-factor authentication.

Context

- You can enable two-factor authentication only for local users, Active Directory (AD)-authenticated users, and Lightweight Directory Access Protocol (LDAP)-authenticated users.
- To enable two-factor authentication for a Resource Access Management (RAM) user, log on to the RAM console and enable multi-factor authentication (MFA). For more information, see Enable an MFA device for an Alibaba Cloud account.

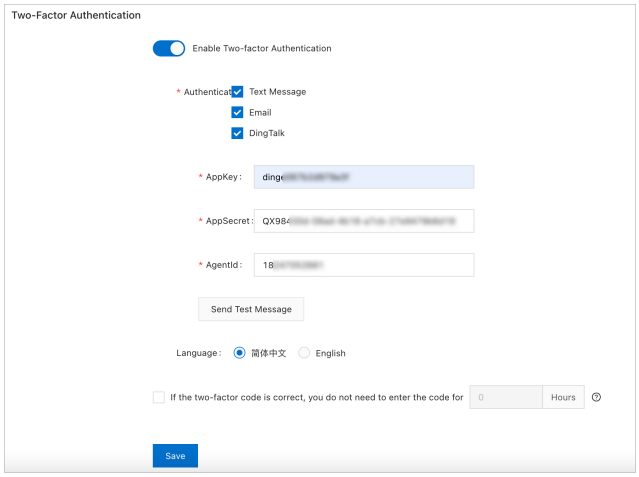
Prerequisites

- If you select Text Message for the Authentication parameter when you enable two-factor authentication, you must specify the mobile phone number of the user who performs O&M operations. If you do not specify the mobile phone number, the user cannot receive verification codes. For more information, see Modify user information.
- If you select Email for the Authentication parameter when you enable two-factor authentication, you must specify the email address of the user who performs O&M operations. If you do not specify the email address, the user cannot receive verification codes. For more information, see Modify user information.
- If you select DingTalk for the Authentication parameter when you enable two-factor authentication, make sure that the following requirements are met:
  - The mobile phone number of the user who performs O&M operations is specified. For more information, see Modify user information.
  - An internal enterprise application is created by the DingTalk administrator, and **the operation that is used to obtain member information based on the mobile phone numbers and names of the members** is activated for the application.
  - The values of **AppKey**, **AppSecret**, and **AgentId** of the internal enterprise application are obtained.

Procedure

1.
2.
3.
4. Turn on **Enable Two-factor Authentication**, configure the parameters, and then click **Save**.

   If you select **DingTalk** for **Authentication**, you must configure **AppKey**, **AppSecret**, and **AgentId** of the internal enterprise application.



1.11.3. Configure AD authentication

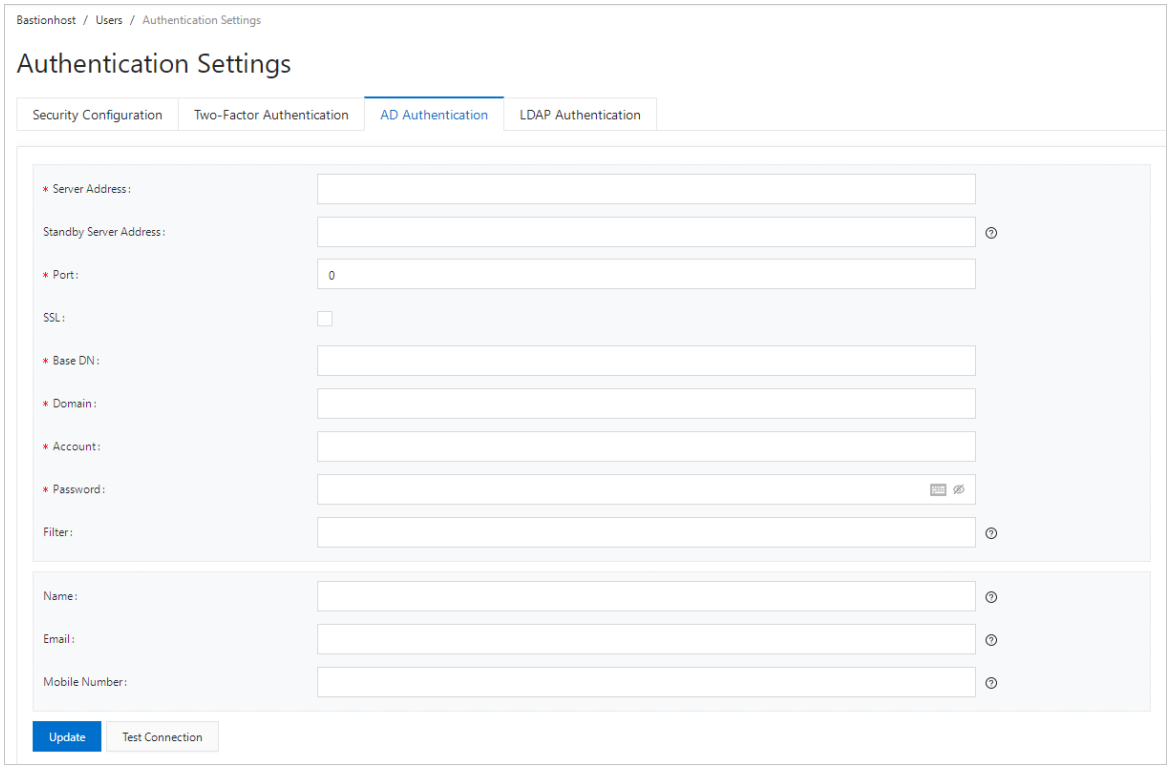
Bastionhost is connected to an AD server, so users on the AD server can be synchronized to Bastionhost as Bastionhost users. Before you synchronize users on the AD server, you must configure AD authentication in the Bastionhost console. This topic describes how to configure AD authentication.

Prerequisites

An AD environment is deployed and Bastionhost can access the AD server.

Procedure

1.
2.
3.
4. Specify parameters on this tab. The required parameters are Server Address, Port, Base DN, Domain, Account, and Password.



5. Click **Test Connection**.
   A message that indicates the operation success is displayed if the test succeeds.
6. Click **Update**.

1.11.4. Configure LDAP authentication

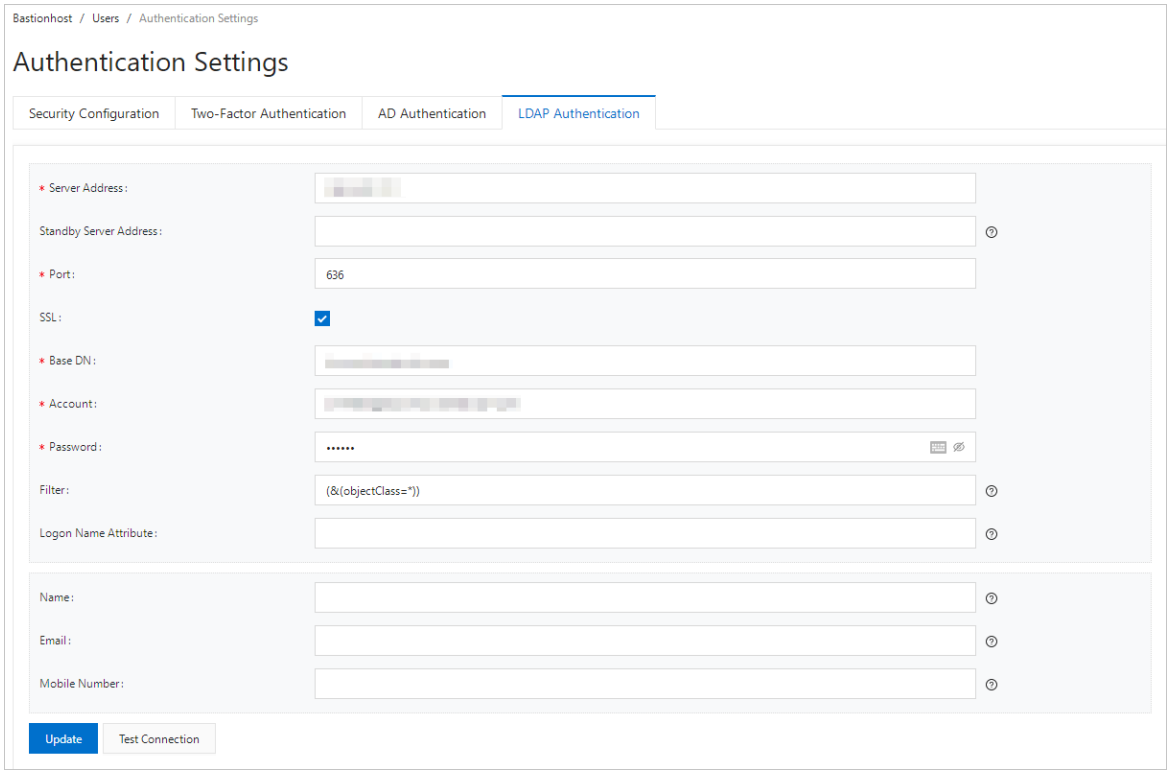
Bastionhost is connected to an LDAP server, so users on the LDAP server can be synchronized to Bastionhost as Bastionhost users. Before you synchronize users on the LDAP server, you must configure LDAP authentication in the Bastionhost console. This topic describes how to configure LDAP authentication.

Prerequisites

An LDAP environment is deployed and Bastionhost can access the LDAP server.

Procedure

1.
2.
3.
4. Specify parameters on this tab. The required parameters are Server Address, Port, Base DN, Account, and Password.



5. Click **Test Connection**.
   A message that indicates the operation success is displayed if the test succeeds.
6. Click **Update**.

1.11.5. Diagnose network issues

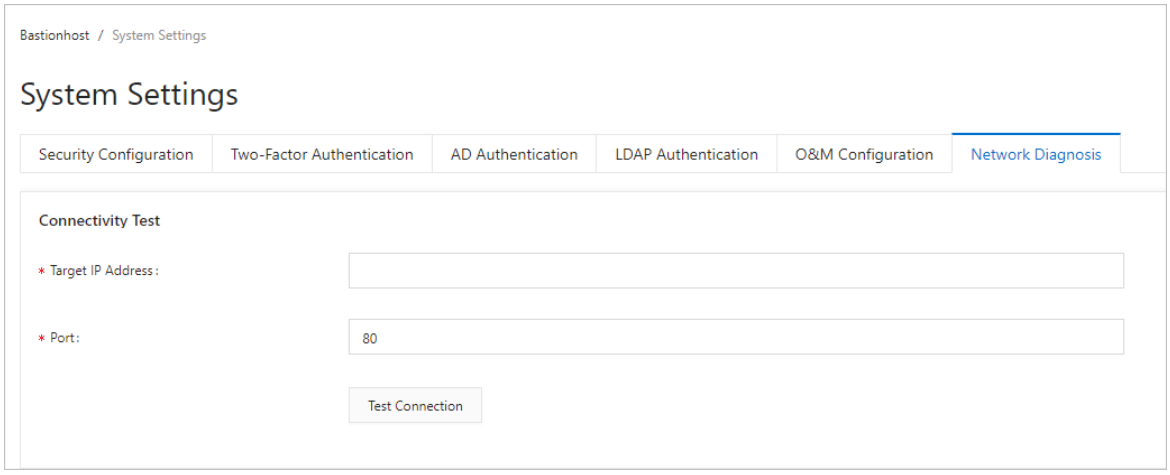
The System Settings page in the Bastionhost console provides a network issue diagnostics feature that allows you to check the connectivity between Bastionhost and specific host ports. You can use this feature to confirm the network accessibility and perform O&M operations more efficiently. This topic describes how to use the network issue diagnostics feature.

Context

The network issue diagnostics feature can detect the connectivity of IPv4 addresses and domain names.

Procedure

1.
2.
3.
4. Specify **Target IP Address** and **Port**.



5. Click **Test Connection**.
   If the connectivity test is successful, the message **The network is connected.** appears. If the connectivity test fails, the message **The network is disconnected.** appears. In this case, you must handle the network connection exception. For more information, see Handle network connection exceptions.

Handle network connection exceptions

If a connectivity test fails, check the following items to identify the cause:

- Check whether the security group rules allow access from Bastionhost to the specific host port.
- Check whether a cloud firewall is deployed for the specific host and whether policies that allow access from Bastionhost to the specific host port are configured.
- Check whether a local firewall is deployed for the specific host and whether policies that allow access from Bastionhost to the specific host port are configured.

1.11.6. Configure O&M settings

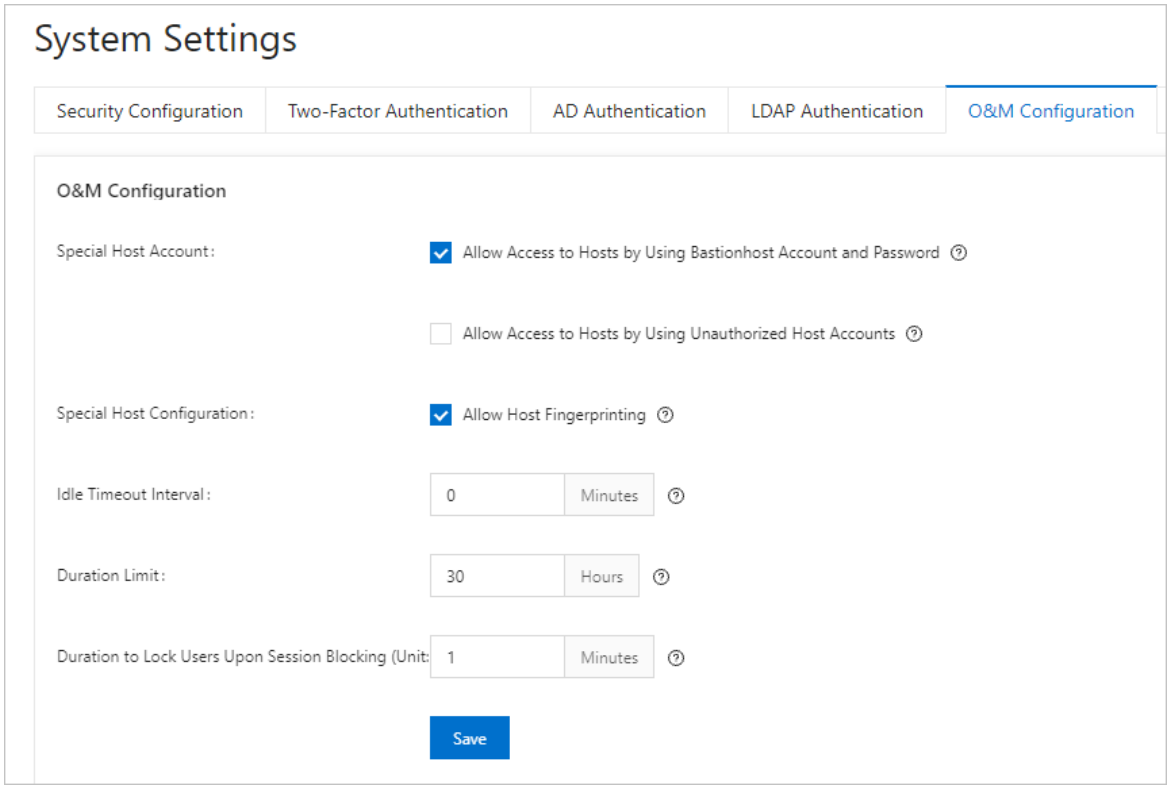
If you want to control the duration of an O&M session, you can configure O&M settings based on your business requirements. This prevents host resources from being wasted due to lengthy O&M sessions or no O&M operations during a long period of time. This topic describes how to configure O&M settings.

Context

You can configure the O&M settings, including Idle Timeout Interval, Duration Limit, and Duration to Lock Users Upon Session Blocking.

Procedure

1.
2.
3.
4. In the **O&M Configuration** section, configure the parameters.



The following table describes the parameters.

Parameter	Description

Parameter	Description
Special Host Account	Valid values: ○ **Allow Access to Hosts by Using Bastionhost Account and Password**: specifies whether to allow users to access hosts by using the username and password of a bastion host. **Note** This configuration is suitable for scenarios in which the bastion host account is imported from Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) servers, the host is in the same domain as the bastion host, and the username and password of the server account are the same as those of the bastion host. ○ **Allow Access to Hosts by Using Unauthorized Host Accounts**: specifies whether to allow password-free access from users to hosts on which the users do not have permissions. This option is selected by default. **Note** This configuration takes effect only when a user accesses hosts on which the user does not have permissions. ■ If a user does not have permissions to access a host, the user can find and select a host that has the user parameter unspecified. Then, the user can enter the username and password of the bastion host to access and perform O&M operations on the host. ■ If this option is cleared, the host account on which the user does not have permissions is not displayed in the asset list during O&M.
Special Host Configuration	Specifies whether to enable the host fingerprint feature. The host fingerprint feature is enabled by default. **Note** A host fingerprint is a unique identifier that Bastionhost uses to identify a Linux host. A host fingerprint can be used to prevent unauthorized users from accessing hosts by redirecting traffic. We recommend that you select Allow Host Fingerprinting.
Idle Timeout Interval	The maximum duration of an idle O&M session. If the duration of an idle O&M session reaches the specified value, the session is automatically disconnected. Valid values: 0 to 60. Unit: minutes. The value 0 indicates that the duration is not limited. **Note** In an **idle O&M session**, a user logs on to a host but does not perform O&M operations.
Duration Limit	The maximum total duration of O&M sessions. If the total duration reaches the specified value, the ongoing sessions are automatically disconnected. Valid values: 0 to 60. Unit: minutes. The value 0 indicates that the duration is not limited.

Parameter	Description
Duration to Lock Users Upon Session Blocking	The time that an O&M session can be interrupted by the administrator. During the specified time, users cannot perform O&M operations on all hosts. Valid values: 0 to 60. Unit: minutes. The value 0 indicates that the time is not limited.

5. After you configure the parameters, click **Save**. The O&M settings are configured.

1.11.7. Use the storage management feature

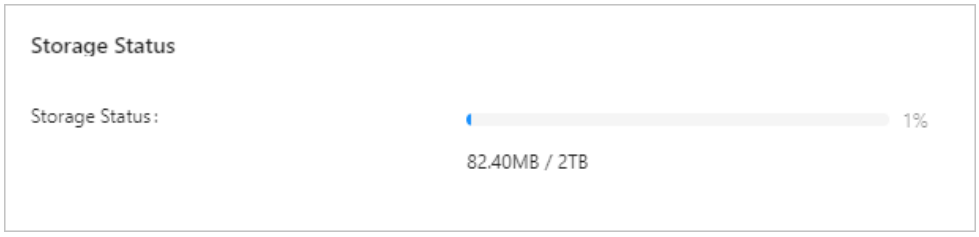
The administrator can use the storage management feature to view the storage occupied by audit session data and specify the storage duration. This topic describes how to use the storage management feature.

Context

After the storage is used up, Bastionhost deletes the audit session data that is stored at the earliest time. We recommend that you specify an appropriate storage duration for audit session data.

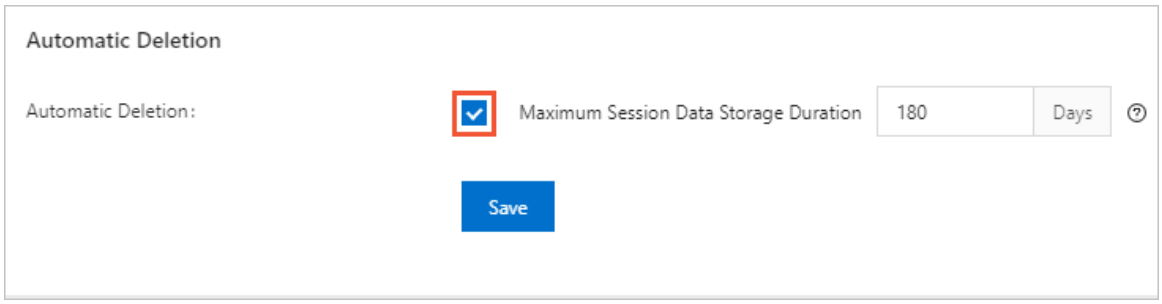
View the storage usage

1.
2.
3. On the **System Settings** page, click the **Storage Management** tab.
4. In the **Storage Status** section, view the storage usage.



Configure automatic deletion of session data

1.
2.
3. In the **Automatic Deletion** section, select **Maximum Session Data Storage Duration**.



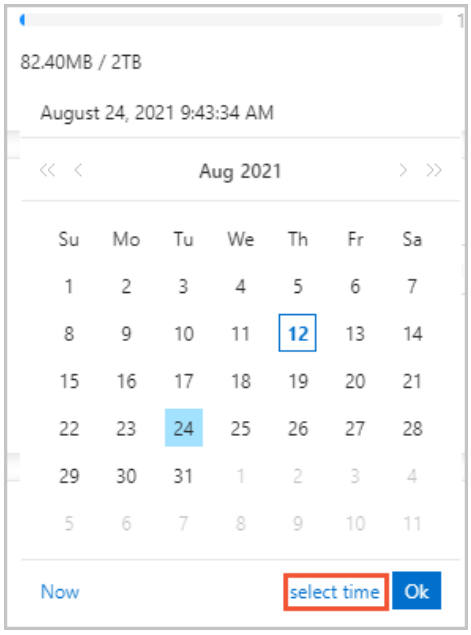
4. Specify a value for **Maximum Session Data Storage Duration** based on your business requirements.

> **Note** Valid values: 1 to 9999. Default value: 180. Unit: days. When the storage is used up, the data stored for a period that exceeds the specified value is automatically deleted.
>
> - If the size of the remaining session data exceeds the maximum storage after the data is deleted, Bastionhost automatically deletes the session data that is stored at the earliest time.
> - If you do not enable automatic deletion, Bastionhost automatically overwrites the data that is stored at the earliest time when the storage is used up.

5. Click **Save**.
   Bastionhost automatically manages the audit session data based on your settings.

Manually delete session data

1.
2.
3. In the **Manual Deletion** section, select a point in time from the date and time picker on the right of **Deleted On**.
4. Click **Ok**.



5. Click **Delete**.
   Bastionhost deletes the audit session data that is stored before the specified point in time.

1.11.8. Use the notification feature

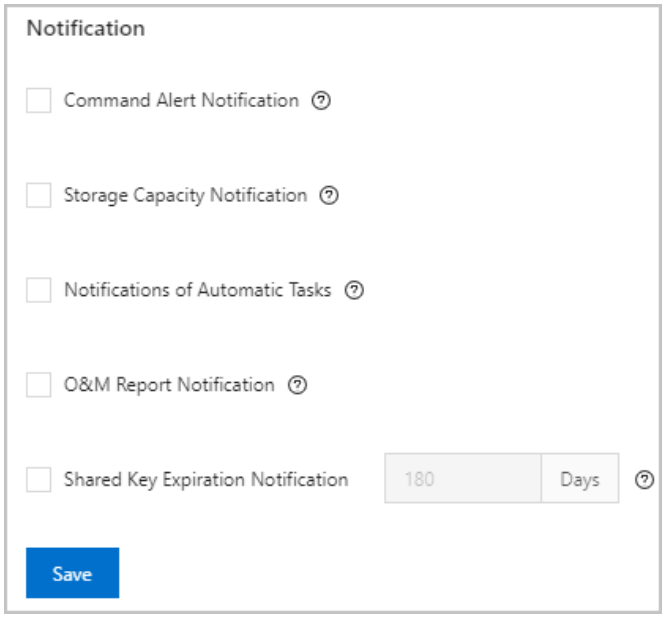
Bastionhost provides the notification feature, which sends you notifications by using internal messages. You can enable the notification feature for the following items: Command Alert Notification, Storage Capacity Notification, Notifications of Automatic Tasks, O&M Report Notification, and Shared Key Expiration Notification. This topic describes how to use the notification feature.

Procedure

1.

2.
3. On the **System Settings** page, click the **Notification** tab.
4. On the **Notification** tab, configure the notification feature.

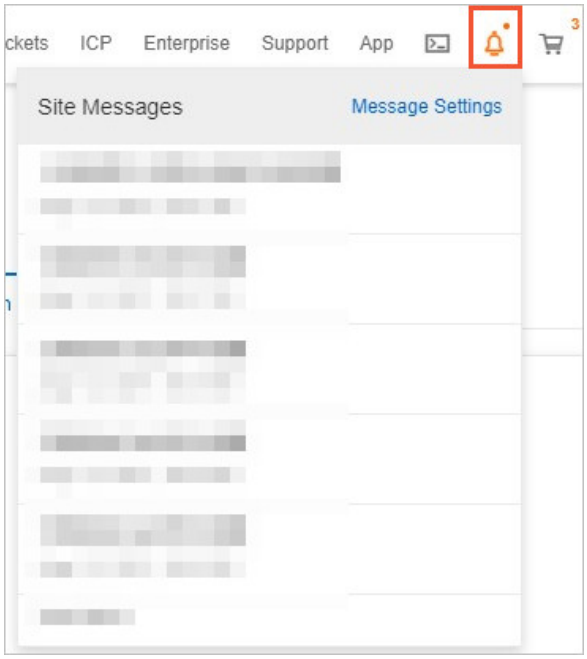
> **Note** By default, the notification feature is disabled for all the items. To allow Bastionhost to send you internal messages for an item, select or configure the item.



Parameter	Description
Command Alert Notification	If an O&M operation triggers a command control policy, Bastionhost notifies you by internal message. Each policy specifies an action on commands, such as approving or blocking commands.
Storage Capacity Notification	If storage space will be used up soon, for example, 85% of the storage space is used, Bastionhost notifies you by internal message. **Note** If the remaining storage space remains unchanged or keeps decreasing, Bastionhost no longer notifies you.
Notifications of Automatic Tasks	If an automatic password change task is complete, Bastionhost notifies you by internal message. **Note** After you create a password change task, Bastionhost automatically runs the task based on the specified time or cycle. The automatic password change feature helps meet the requirements of classified protection and prevents errors caused by regular and manual password rotation. For more information about how to create an automatic password change task, see Use the automatic password change feature.

Parameter	Description
O&M Report Notification	On each Monday, Bastionhost sends you the O&M reports of the last week by internal message.
Shared Key Expiration Notification	If a period is set for this parameter, Bastionhost notifies you of changing the shared key by internal message when the shared key is about to expire. Only a Bastionhost administrator can set the period. **Note** After you create a shared key and associate the key with multiple host accounts, the shared key is preferentially used to log on to the hosts for O&M. This makes the host account management more efficient. For more information about how to create a shared key, see Use the key management feature.

5. Click **Save**.
   Bastionhost sends you notifications by using internal messages based on your configurations. You can click the icon in the upper-right corner of the Bastionhost console to go to the **Message Center**. In the Message Center, you can view your notifications.



1.11.9. Use the configuration backup feature

Bastionhost provides the configuration backup feature. You can use the feature to replicate the configurations of an existing bastion host to a new bastion host. This way, you do not need to repeat the configuration steps on the new bastion host. This topic describes how to use the configuration backup feature.

Limits

- You can import the configurations from a bastion host that has low specifications to another bastion

host that has the same specifications or a bastion host that has high specifications. For example, you can import the configurations of a bastion host that can manage 50 assets to a bastion host that can manage 200 assets. You cannot import the configurations of a bastion host that can manage 200 assets to a bastion host that can manage 50 assets.

- You can import the configurations from a bastion host to another bastion host of the same edition. For example, you can import the configurations from a bastion host of the Basic edition to another bastion host of the Basic edition.
- You can import the configurations from a bastion host of the low edition to a bastion host of the high edition. For example, you can import the configurations from a bastion host of the Basic edition to a bastion host of the edition.
- You cannot import the configurations from a bastion host of the edition to a bastion host of the Basic edition.
- You cannot export the configurations of a password change task. If you want to run a password change task on a new bastion host, you must configure the task on the new bastion host. You must terminate the password change task on an existing bastion host and keep the new password in a secure manner.

Procedure

After you purchase a new bastion host, you can export a configuration backup file of an existing bastion host to your computer by using the configuration backup feature, and upload the configuration backup file to the new bastion host. To upload the exported configuration backup file, perform the following steps:

1. Create a configuration backup task for the existing bastion host and export the configuration backup file. For more information, see Create a configuration backup task.
2. Upload the configuration backup file that you exported to the new bastion host. For more information, see Upload the configuration backup file.

Create a configuration backup task

1.
2. In the left-side navigation pane, click **System Settings**.
3. On the **System Settings** page, click the **Configuration Backup File** tab.
4. On the **Configuration Backup File** tab, click **Create Configuration Backup**.

   The configuration backup file of the bastion host is downloaded to your computer in the .bh format.

Upload the configuration backup file

Notice After you import the configurations to the new bastion host, the configurations of the new bastion host are overwritten. Proceed with caution.

1.
2. In the left-side navigation pane, click **System Settings**.
3. On the **System Settings** page, click the **Configuration Backup File** tab.
4. On the **Configuration Backup File** tab, click **Upload**.

   After you upload the configuration backup file, you can check whether the configurations are uploaded to the new bastion host and view the uploaded configurations.

1.11.10. Manage third-party asset sources

After you add a third-party asset source to Bastionhost, Bastionhost can call the operation that is provided by the third-party asset source to obtain the hosts that belong to the third-party asset source. You can import the hosts from the third-party asset source to Bastionhost and perform O&M operations on the hosts. This topic describes how to manage third-party asset sources.

Prerequisites

- An asset source that is created by a third-party service provider is used, and hosts are added to the asset source.
- The access credentials (Access Key ID and Secret Access Key) of the third-party asset source are obtained, and the access credentials have the read permissions on host information. For more information, see the official documentation of the third-party service provider.

> **Note** Only specific third-party asset sources are supported. You can submit a ticket to inquire about the supported third-party asset sources.

Import a third-party asset source

1.
2.
3. On the **System Settings** page, click the **Third-party Hosts** tab.
4. On the **Third-party Hosts** tab, click **Import Third-party Host**.
5. In the **Import Third-party Host** panel, configure the parameters and click **Create**.

Parameter	Description
Host Name	Specify a name for the asset source. The name must be 1 to 128 characters in length and can contain letters, digits, periods (.), underscores (_), hyphens (-), backslashes (\), and spaces. The name cannot start with a special character.
Third-party Provider	Select the third-party service provider to which the asset source belongs.
Access Key ID	Enter the Access Key ID of the third-party asset source.
Secret Access Key	Enter the Secret Access Key of the third-party asset source.

What to do next

After you import a third-party asset source, you can import the hosts from the third-party asset source. For more information, see Import a host from a third-party asset source.

Related operations

- Update the information about a third-party asset source. If the information about a third-party asset source is changed, you can update the information to obtain the most recent host information.

  On the **Third-party Hosts** tab, find the required third-party asset source and click **Synchronize** in the **Actions** column.

- Modify the information about a third-party asset source. You can modify the name, service provider, Access Key ID, and Secret Access Key of a third-party asset source.

  On the **Third-party Hosts** tab, find the required third-party asset source and click its name. In the **Modify Information About Third-party Host** panel, modify the information and click **Edit**.

- Delete a third-party asset source. You can delete the third-party asset source that you no longer use.

  On the **Third-party Hosts** tab, find the required third-party asset source and click **Delete** in the **Actions** column. In the message that appears, click **Delete**.

  > **Notice** Before you delete a third-party asset source, make sure that all hosts that belong to the asset source are deleted. If a host exists in the third-party asset source, you cannot delete the third-party asset source. For more information, see Delete a host.

2.O&M manual

2.1. O&M overview

This topic describes the O&M methods that are supported by Bastionhost and how to use Bastionhost to perform O&M operations on servers. This topic is intended for O&M personnel. Bastionhost supports two methods to perform O&M operations: client-based O&M and web-based O&M. We recommend that you choose a method based on your daily O&M requirements.

Web-based O&M

Bastionhost allows you to perform O&M operations on a web page. You do not need to download an O&M client. You can log on to a server from your browser to perform O&M operations on a web page. To log on to the server, use the host O&M feature in the Bastionhost console. For more information, see Use the host O&M feature.

Client-based O&M

You can download the O&M client for the operating system that you use and log on to your bastion host to perform O&M operations on your server.

Windows client-based O&M

- SSH-based O&M
- RDP-based O&M
- Perform SFTP-based O&M

macOS client-based O&M

- SSH-based O&M
- RDP-based O&M
- Perform SFTP-based O&M

2.2. Windows client-based O&M

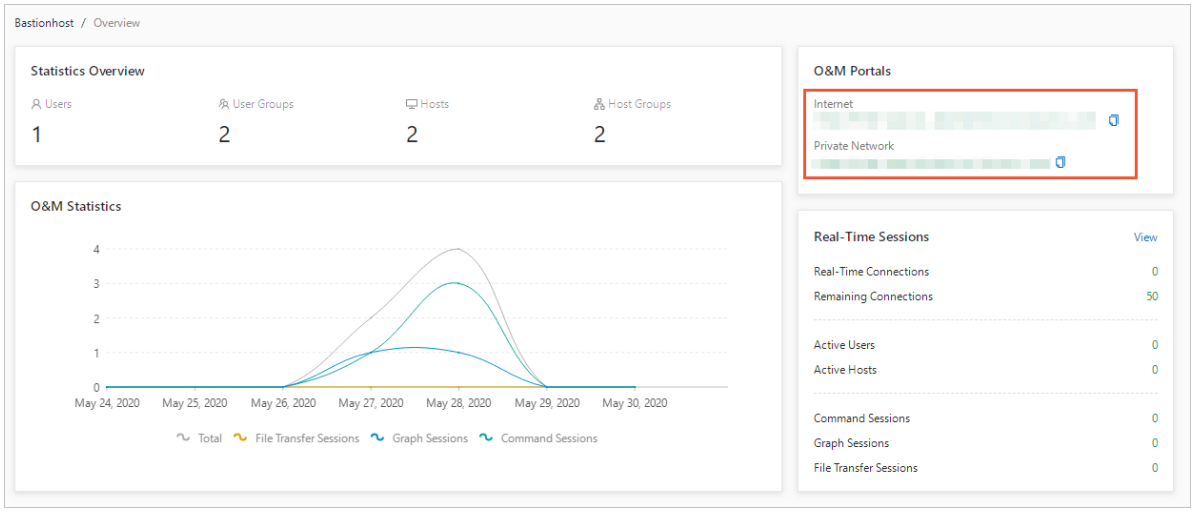
2.2.1. SSH-based O&M

This topic describes how to use a local SSH client tool to log on to Bastionhost and access a host for which you want to perform O&M operations. Xshell is used as an example.

Prerequisites

- An O&M tool that supports SSH, such as Xshell, SecureCRT, or PuTTY, is installed on your local host.

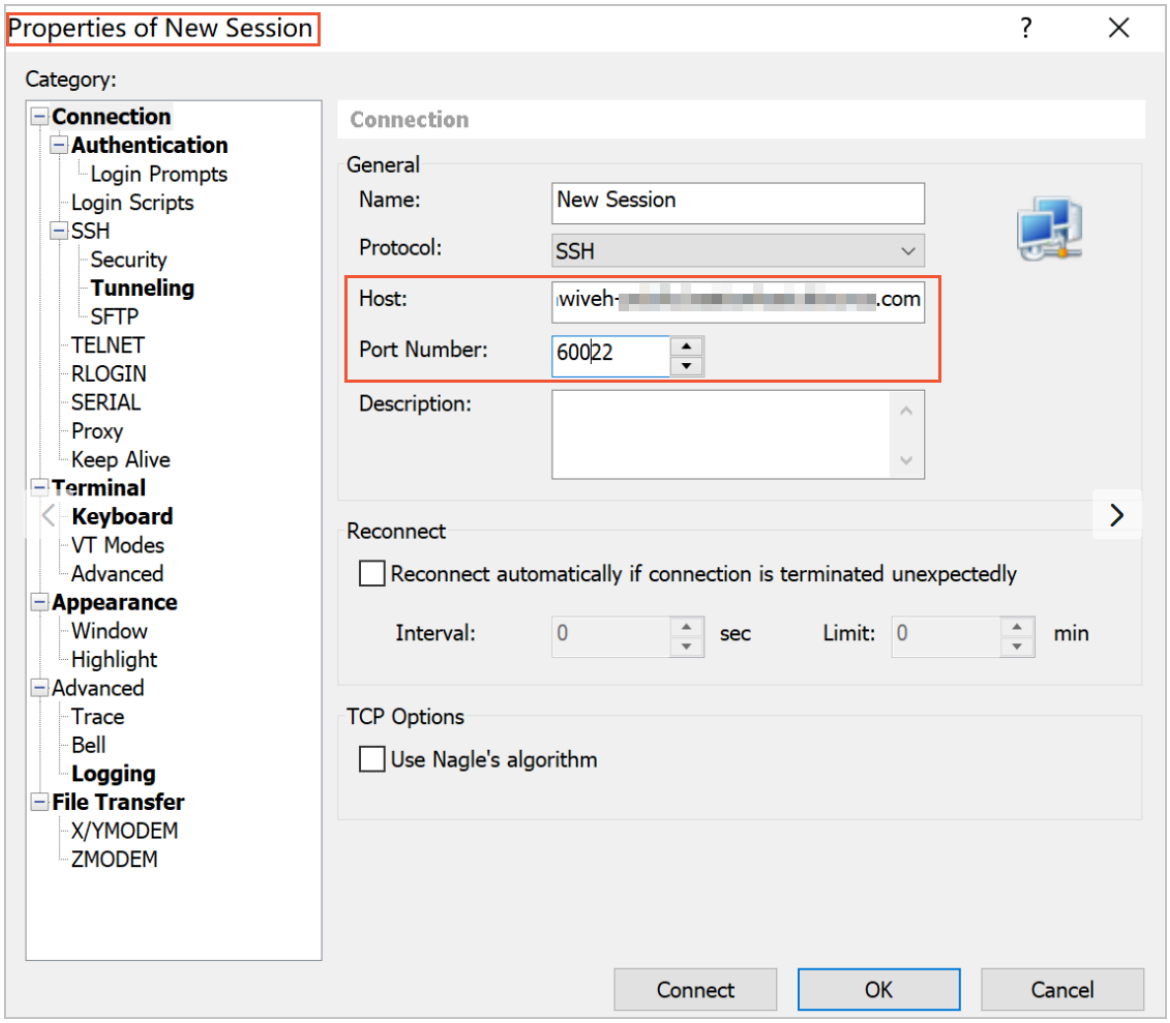
- Bastionhost O&M addresses are obtained. You can obtain these addresses in the **O&M Portals** section on the **Overview** page of Bastionhost. For more information, see Log on to a bastion host.



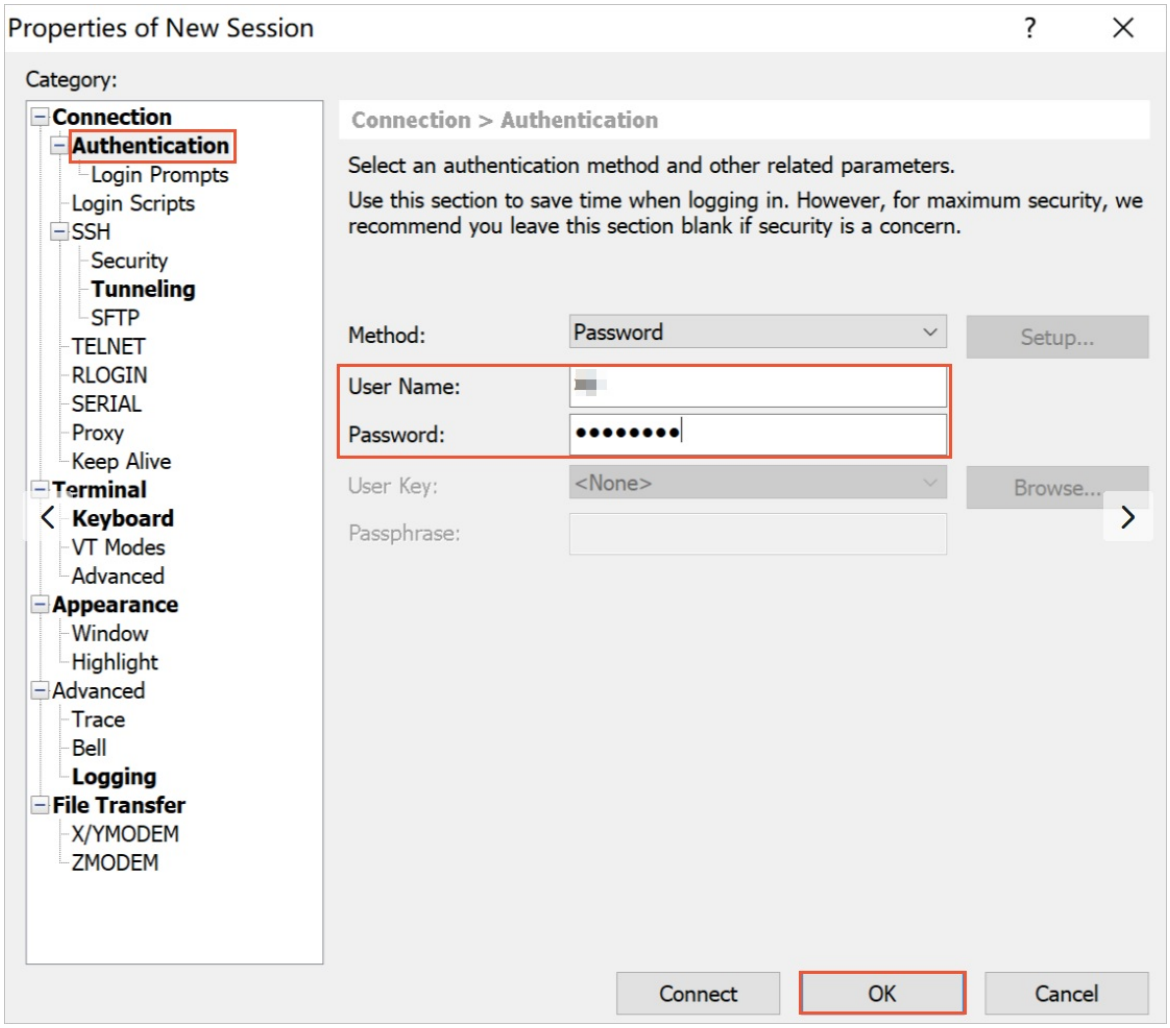
Procedure

1. Start the Xshell tool. Click the New icon on the File menu. In the Properties of New Session dialog box that appears, click **Connection** in the left-side navigation pane and enter a Bastionhost O&M address and an SSH port number in the General section.

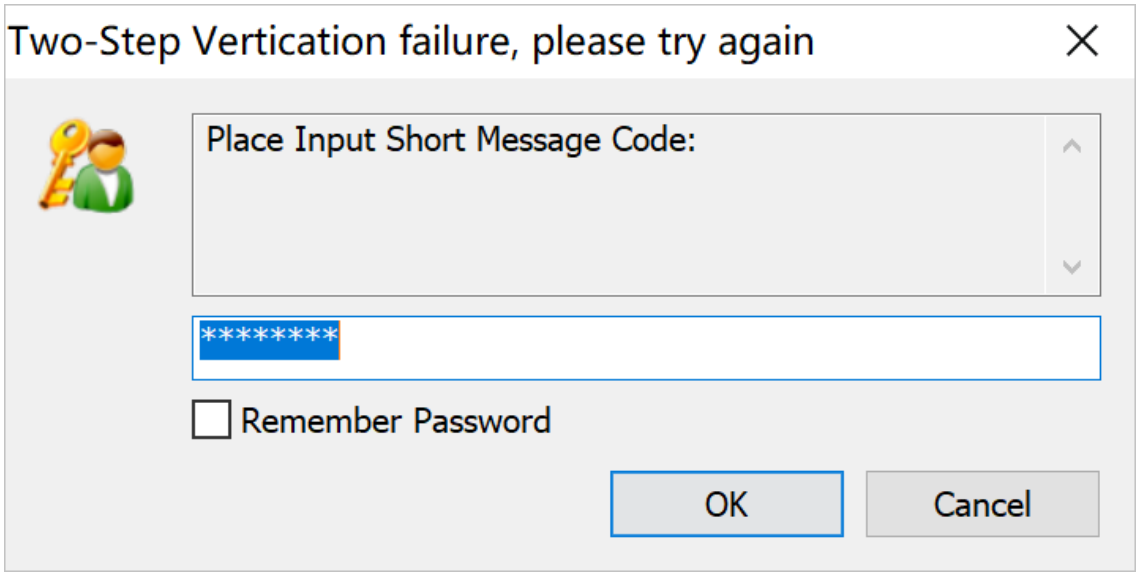
   The SSH port number is **60022** by default.



2. Choose **Connection** > **Authentication** in the left-side navigation pane, enter the username and password used to access Bastionhost, and click **OK**.

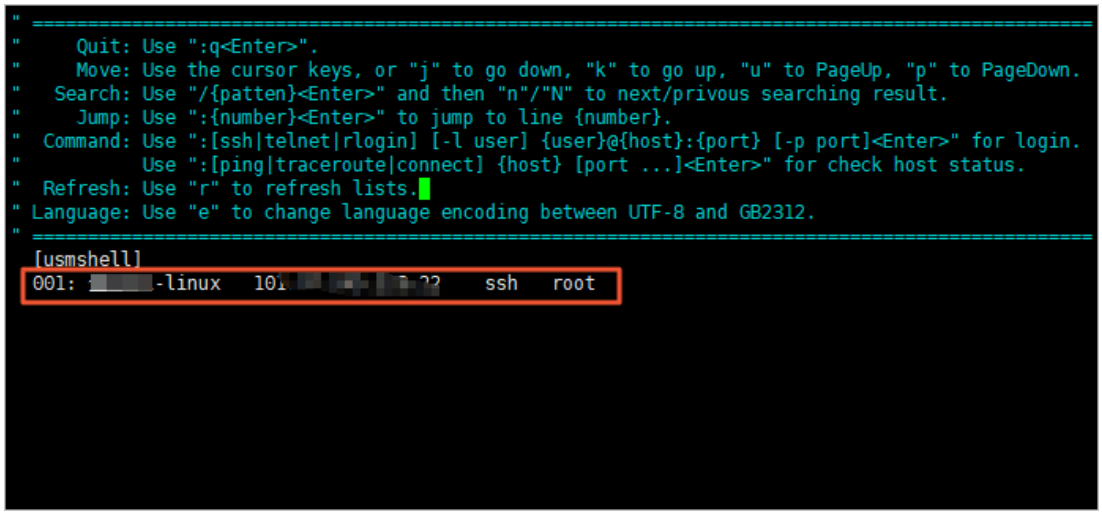


3. (Optional)If multi-factor authentication (MFA) is enabled for a RAM user, enter the verification code obtained from the bound MFA device (the Alibaba Cloud app) in the two-step verification dialog box that appears and click **OK**.



4. On the asset management page that appears, select the host for which you want to perform O&M operations by pressing the upward or downward arrow key, and press Enter to access the target

host for O&M.

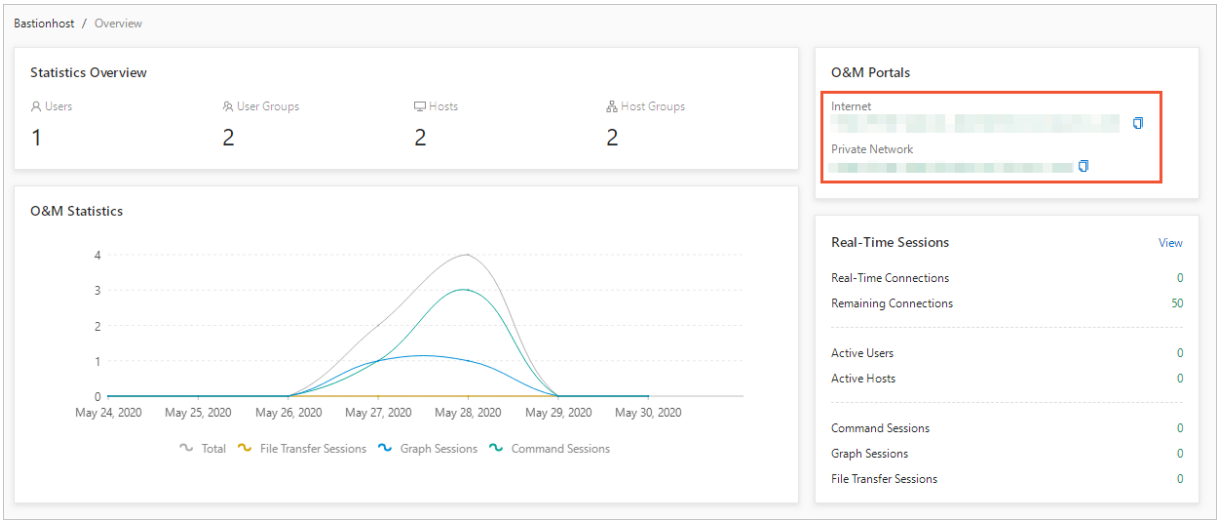


2.2.2. RDP-based O&M

This topic describes how to use a local RDP client tool to log on to Bastionhost and access a host for which you want to perform O&M operations. A built-in Remote Desktop Connection (RDC) (formerly MSTSC) is used as an example.

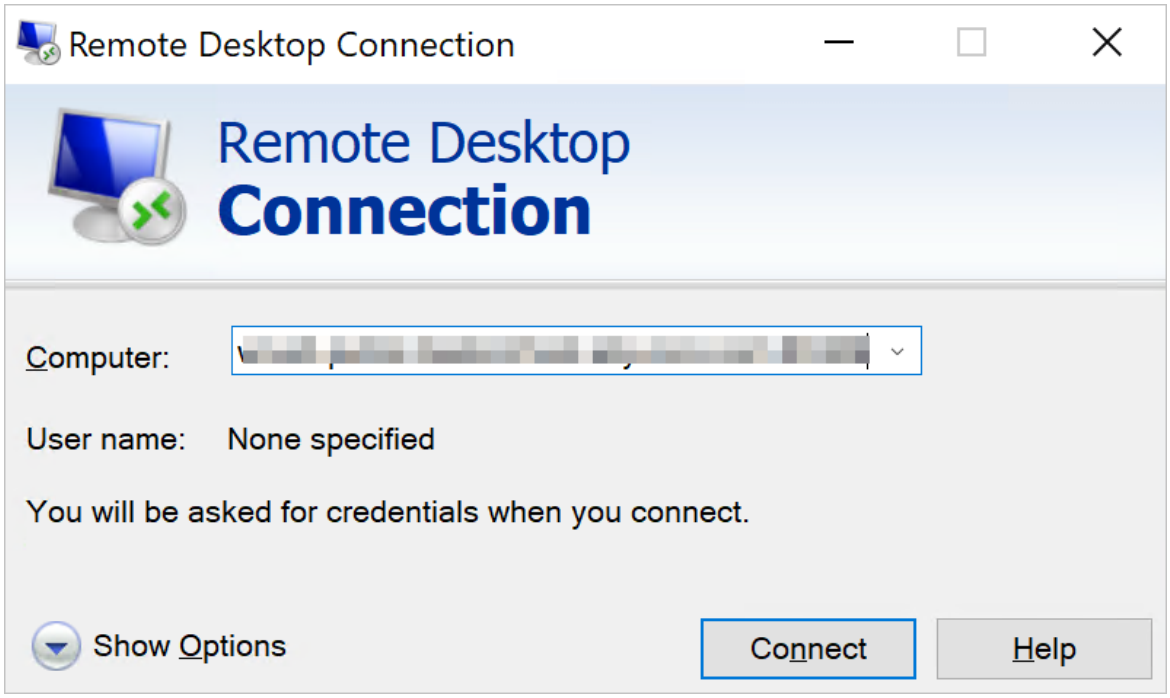
Prerequisites

Bastionhost O&M addresses are obtained. You can obtain these addresses in the **O&M Portals** section on the **Overview** page of Bastionhost. For more information, see Log on to a bastion host.

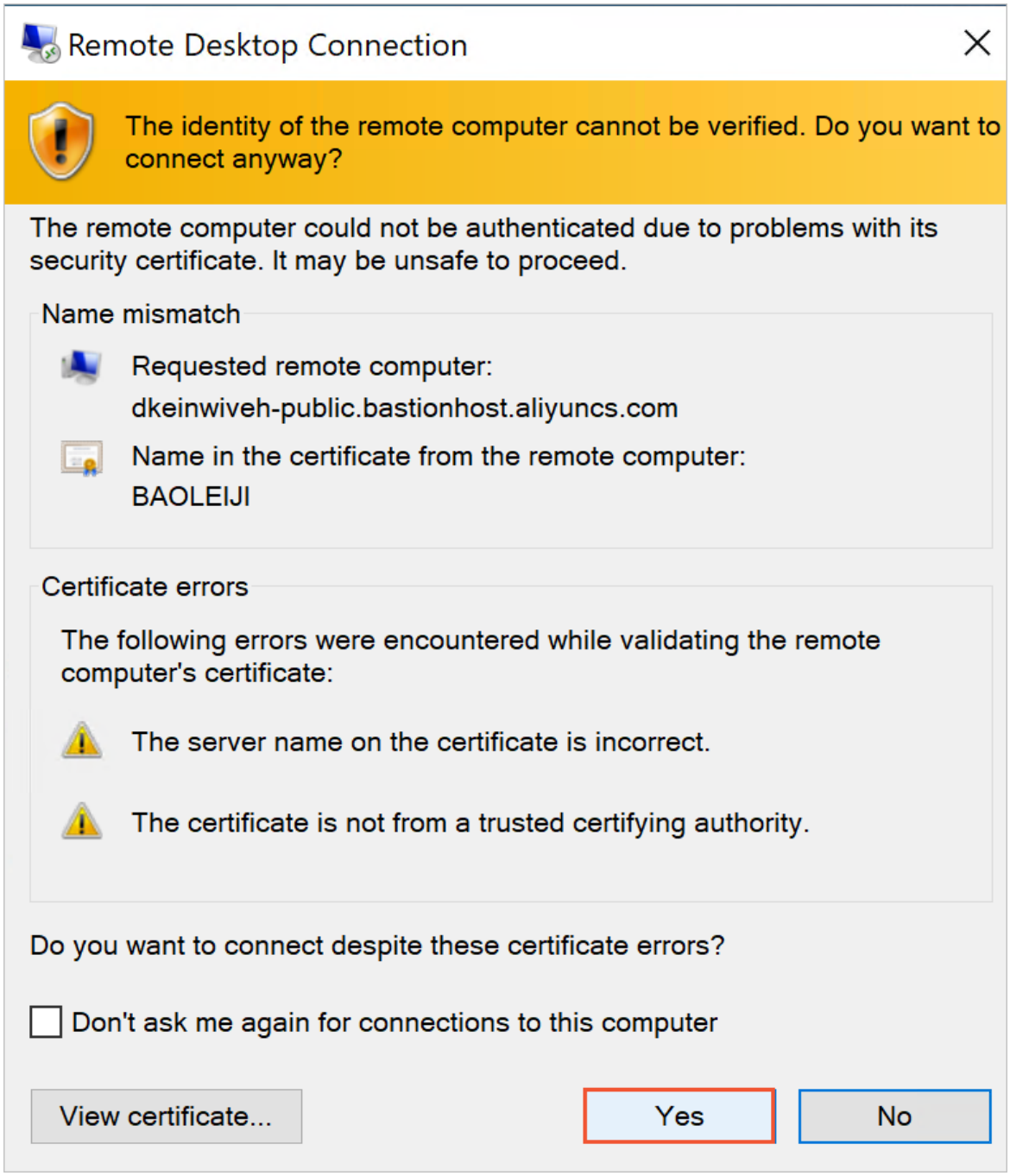


Procedure

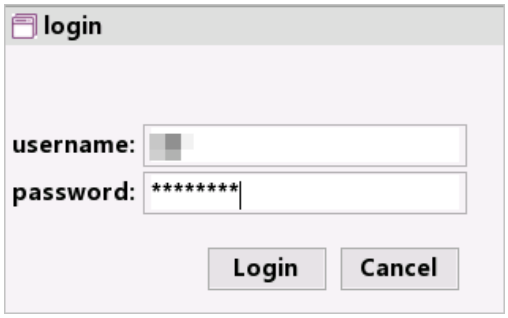
1. Start RDC on your local host.
2. Enter `<Bastionhost O&M address>:63389` and click **Connect**.



3. In the **Remote Desktop Connection** dialog box that appears, click **Yes**.

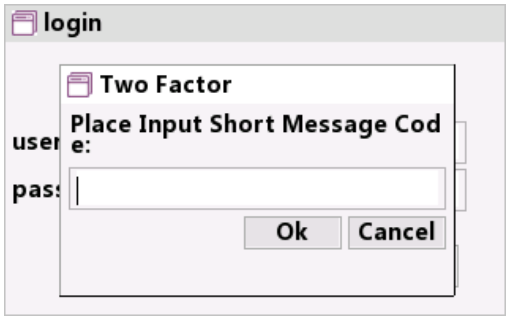


4. In the login dialog box that appears, enter the username and password used to access Bastionhost and click **Login**.

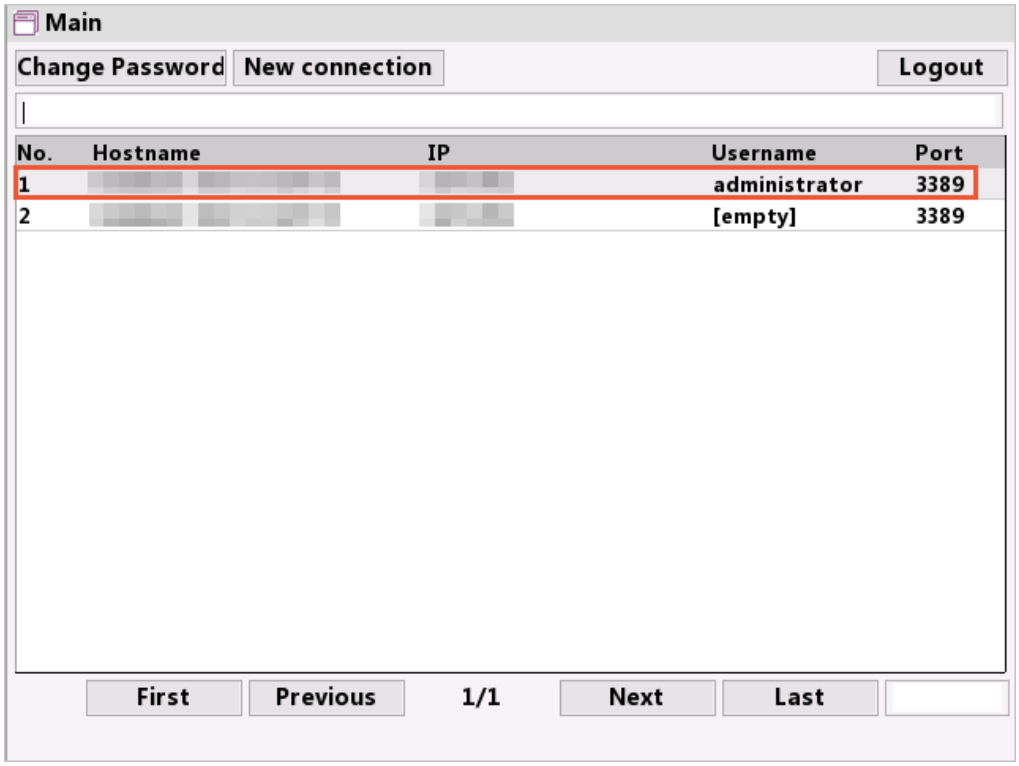


5. (Optional)If multi-factor authentication (MFA) is enabled for a RAM user, enter the verification code

obtained from the bound MFA device (the Alibaba Cloud app) in the Two Factor dialog box that appears and click **Ok**.



6. On the asset management page, double-click the authorized host that you want to access for O&M.



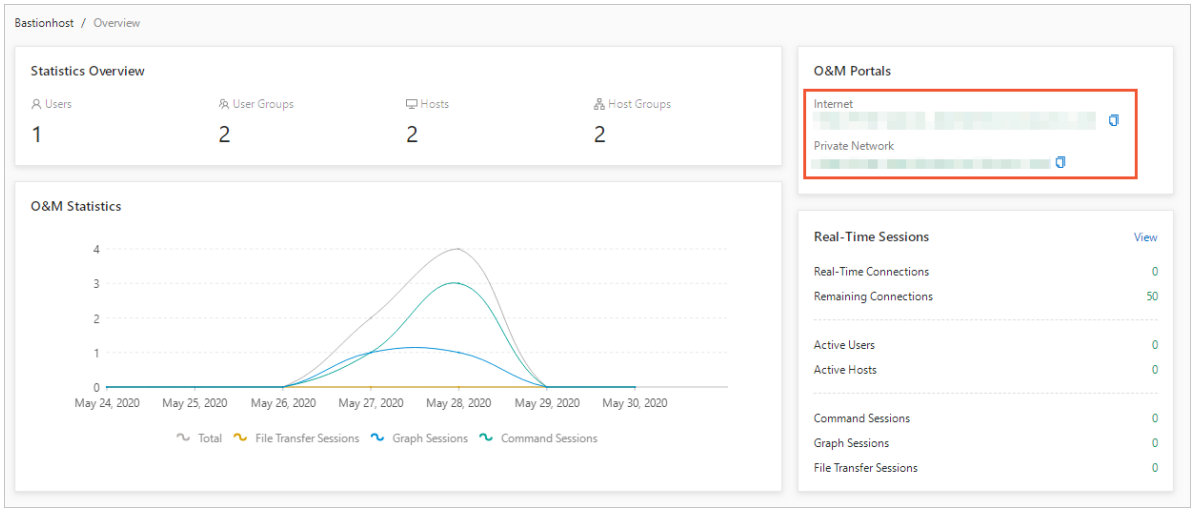
2.2.3. Perform SFTP-based O&M

This topic describes how to use an SFTP client tool on your computer to log on to a bastion host and access a host for which you want to perform O&M operations. In this example, Xftp is used.

Prerequisites

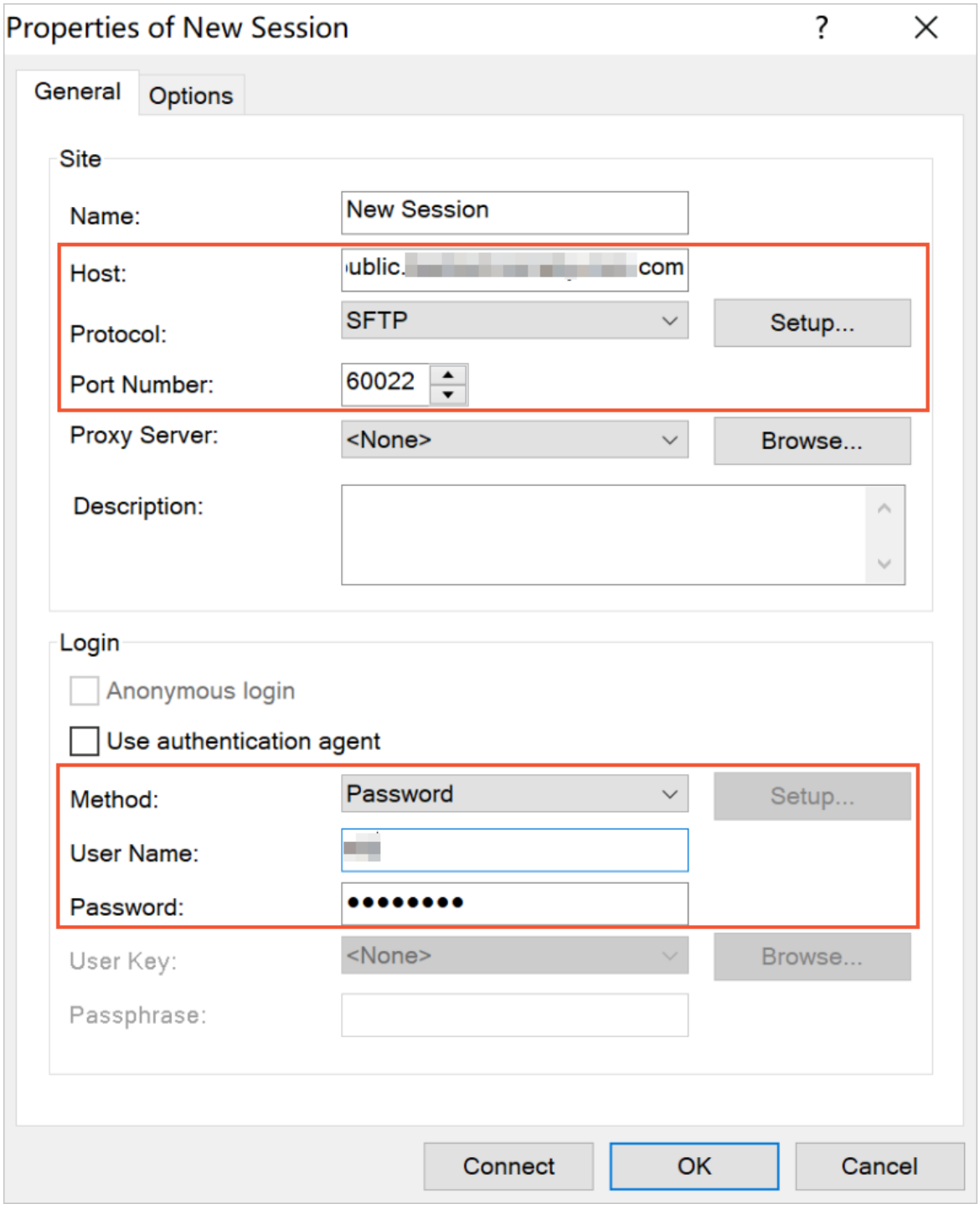
- An O&M tool that supports SFTP, such as Xftp or WinSCP, is installed on your computer.

- Bastionhost O&M addresses are obtained. You can obtain these addresses in the **O&M Portals** section on the **Overview** page of Bastionhost. For more information, see Log on to a bastion host.

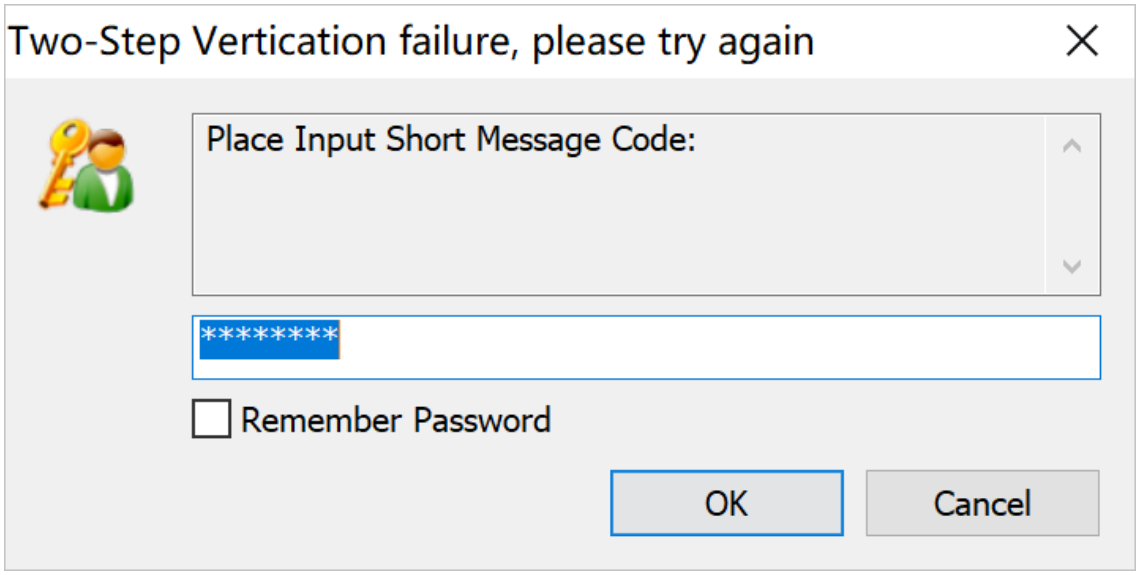


Procedure

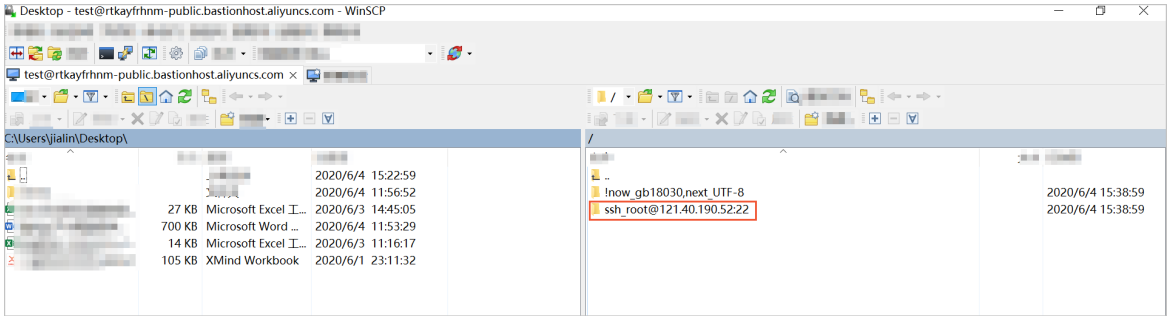
1. Start the Xftp tool. Click the New icon on the File menu. In the Properties of New Session dialog box, enter the O&M address of the bastion host, the default port number 60022, and the username and password to access the bastion host on the General tab. Then click **OK** to connect to the bastion host.



2. (Optional)If multi-factor authentication (MFA) is enabled for a RAM user, enter the verification code that you obtained from the bound MFA device (the Alibaba Cloud app) in the Two-Step Verification dialog box and click **OK**.



3. After you log on to the bastion host, view the hosts that you can manage on the right.



4. Double-click the host for which you want to perform O&M operations to access the host directory and transfer files.

> **Note** If you cannot access the host directory, use one of the following methods to resolve the issue:
>
> - Check whether the username and password of the host are managed in Bastionhost. If the username and password of the host are not configured in Bastionhost, configure the username and password of the host. For more information, see Create an account for a host.
> - Check whether the name of the host directory is garbled. If the name of the host directory is garbled, you can double-click a transcoding directory and ignore the error message. Then, you can right-click the blank space and select Refresh to transcode the garbled directory name.
> - Clear the cache on Xftp. For example, if you use Xftp 6.0, you can click **Options** in the menu bar. In the Options dialog box, click the **Security** tab. In the **History** section, click **Clear**.
>
> If none of the preceding methods resolve your issue, submit a .

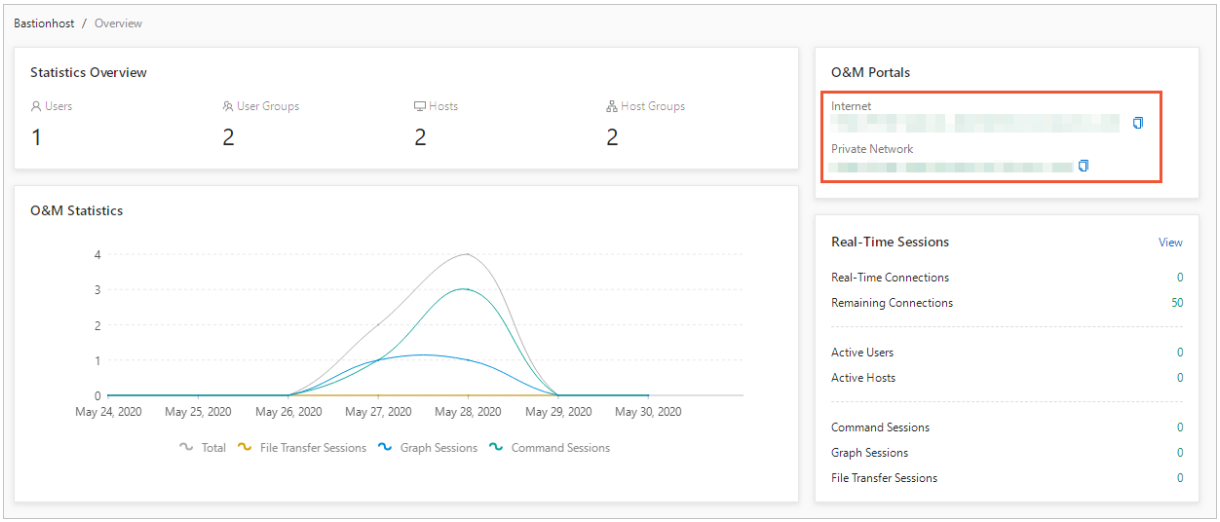
2.3. macOS client-based O&M

2.3.1. SSH-based O&M

This topic describes how to use an SSH tool to log on to Bastionhost and access a host for which you want to perform O&M operations. A command-line tool is used as an example.

Prerequisites

Bastionhost O&M addresses are obtained. You can obtain these addresses in the **O&M Portals** section on the **Overview** page of Bastionhost. For more information, see Log on to a bastion host.

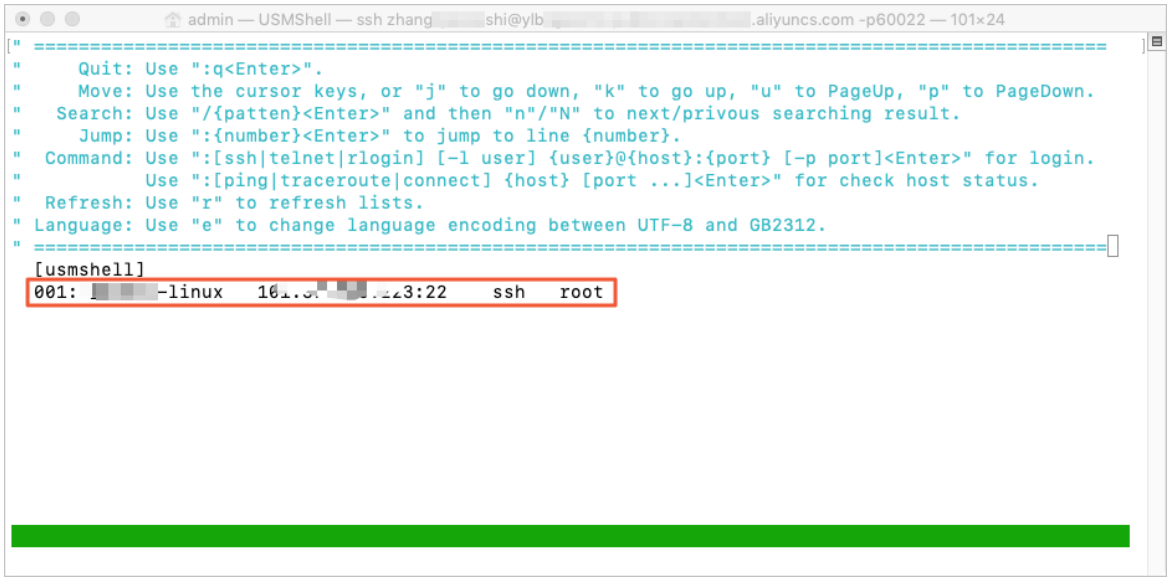


Procedure

1. Start the command-line tool.
2. Type `ssh <Username to access Bastionhost>@<Bastionhost O&M address> -p60022` and press Enter.

3. Type the password of a RAM user and press Enter.
4. (Optional)If multi-factor authentication (MFA) is enabled for the RAM user, type the verification code obtained from the bound MFA device (the Alibaba Cloud app) and press Enter.

5. On the asset management page that appears, select the host for which you want to perform O&M operations by pressing the upward or downward arrow key, and press Enter to access the target host for O&M.

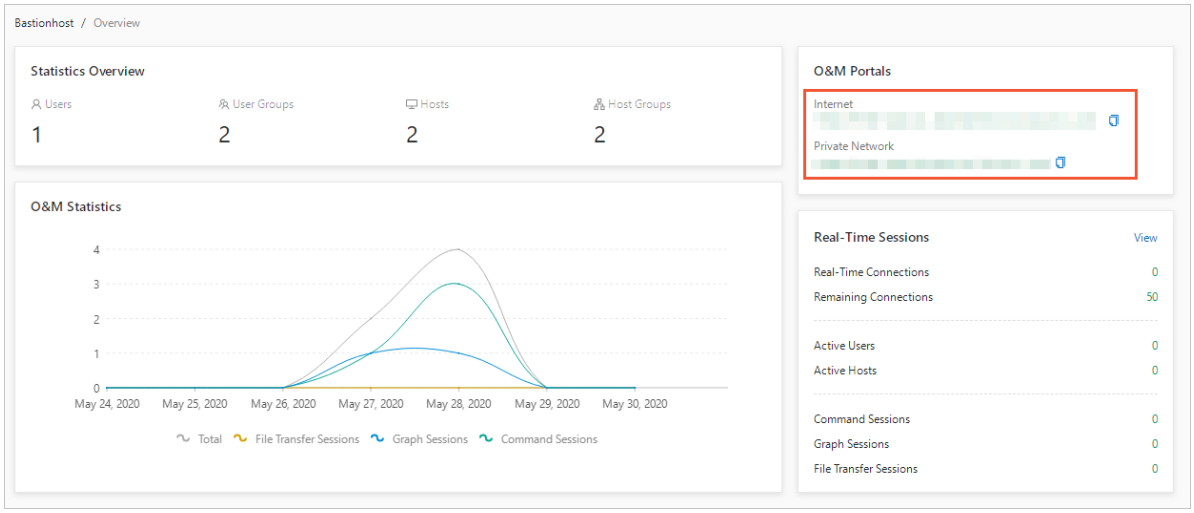


2.3.2. RDP-based O&M

This topic describes how to use a local RDP client tool to log on to Bastionhost and access a host for which you want to perform O&M operations. The Microsoft Remote Desktop application is used as an example.

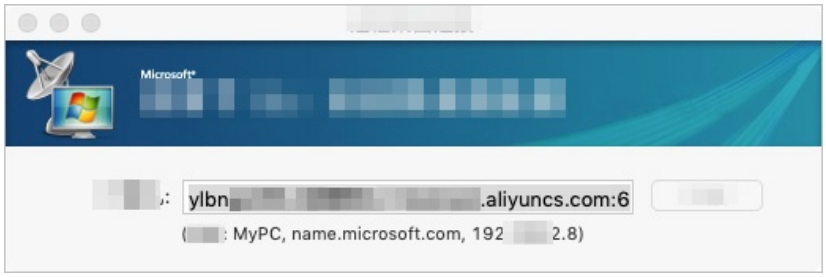
Prerequisites

- The Microsoft Remote Desktop application is downloaded from Microsoft Store and installed on your local host.
- Bastionhost O&M addresses are obtained. You can obtain these addresses in the **O&M Portals** section on the **Overview** page of Bastionhost. For more information, see Log on to a bastion host.

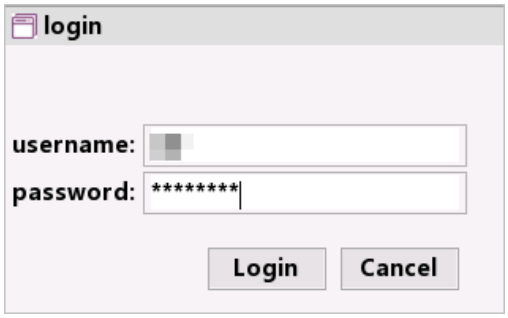


Procedure

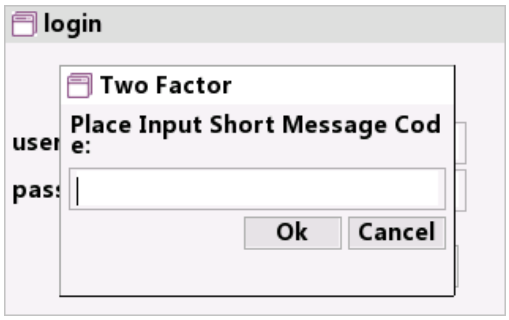
1. Start Microsoft Remote Desktop.
2. Enter `<Bastionhost O&M address>:63389` in the Computer field and click **Connect**.



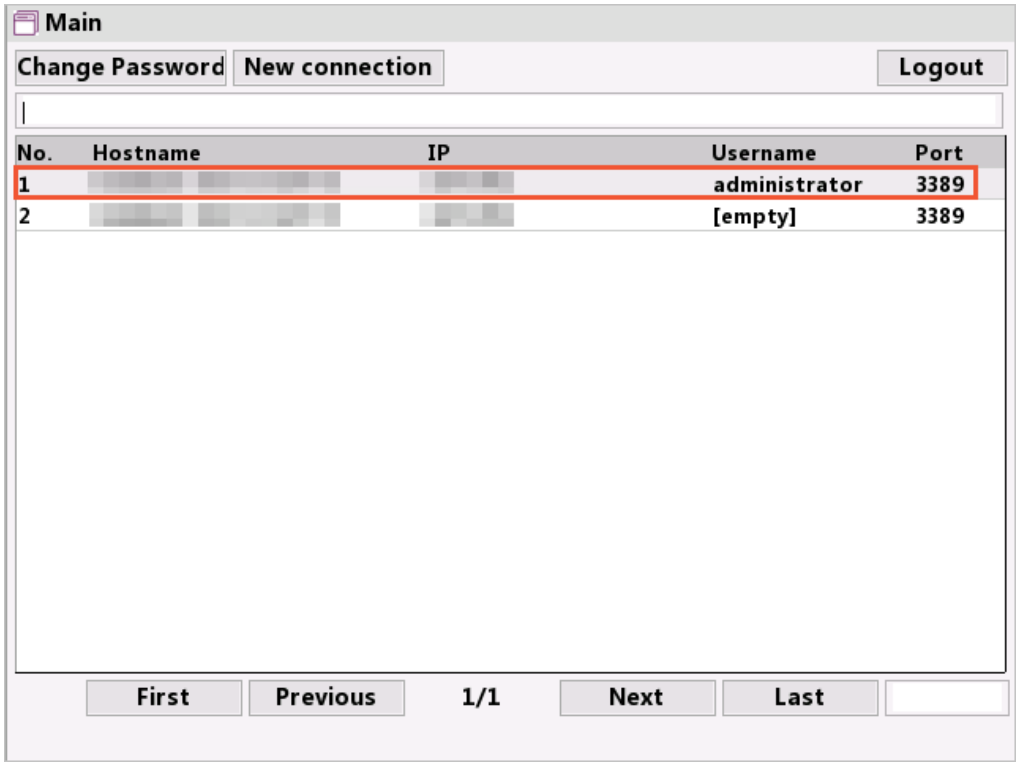
3. In the login dialog box that appears, enter the username and password used to access Bastionhost and click **Login**.



4. (Optional)If multi-factor authentication (MFA) is enabled for a RAM user, enter the verification code obtained from the bound MFA device (the Alibaba Cloud app) in the Two Factor dialog box that appears and click **Ok**.



5. On the asset management page, double-click the authorized host that you want to access for O&M.

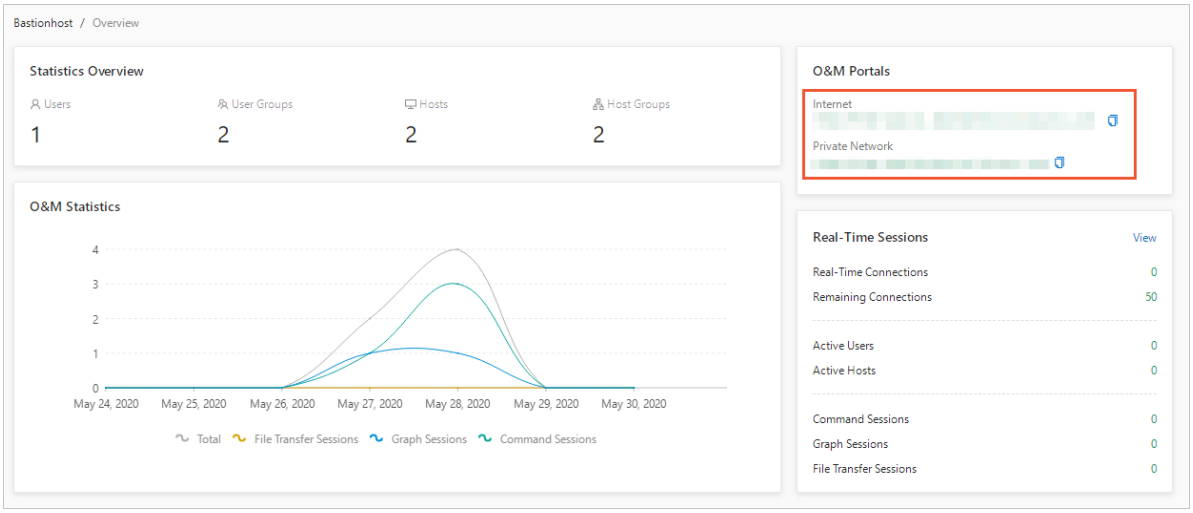


2.3.3. Perform SFTP-based O&M

This topic describes how to use an SFTP client tool on your computer to log on to a bastion host and access a host for which you want to perform O&M operations. In this example, SecureFX is used.

Prerequisites

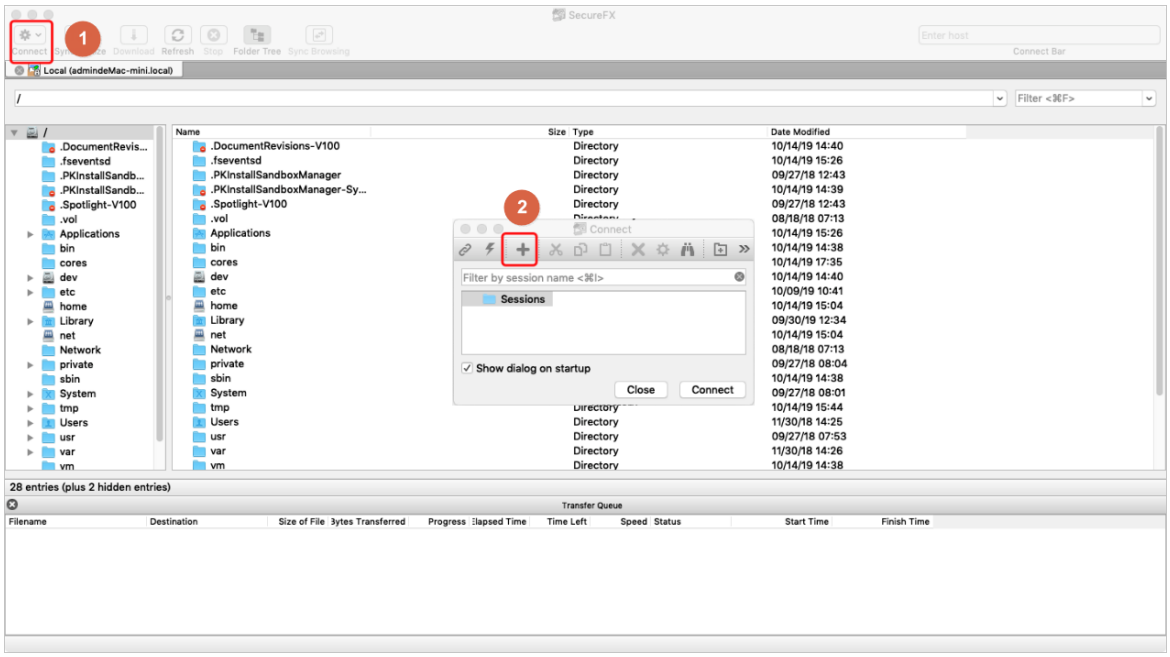
- An O&M tool that supports SFTP, such as SecureFX, is installed on your computer.
- Bastionhost O&M addresses are obtained. You can obtain these addresses in the **O&M Portals** section on the **Overview** page of Bastionhost. For more information, see Log on to a bastion host.



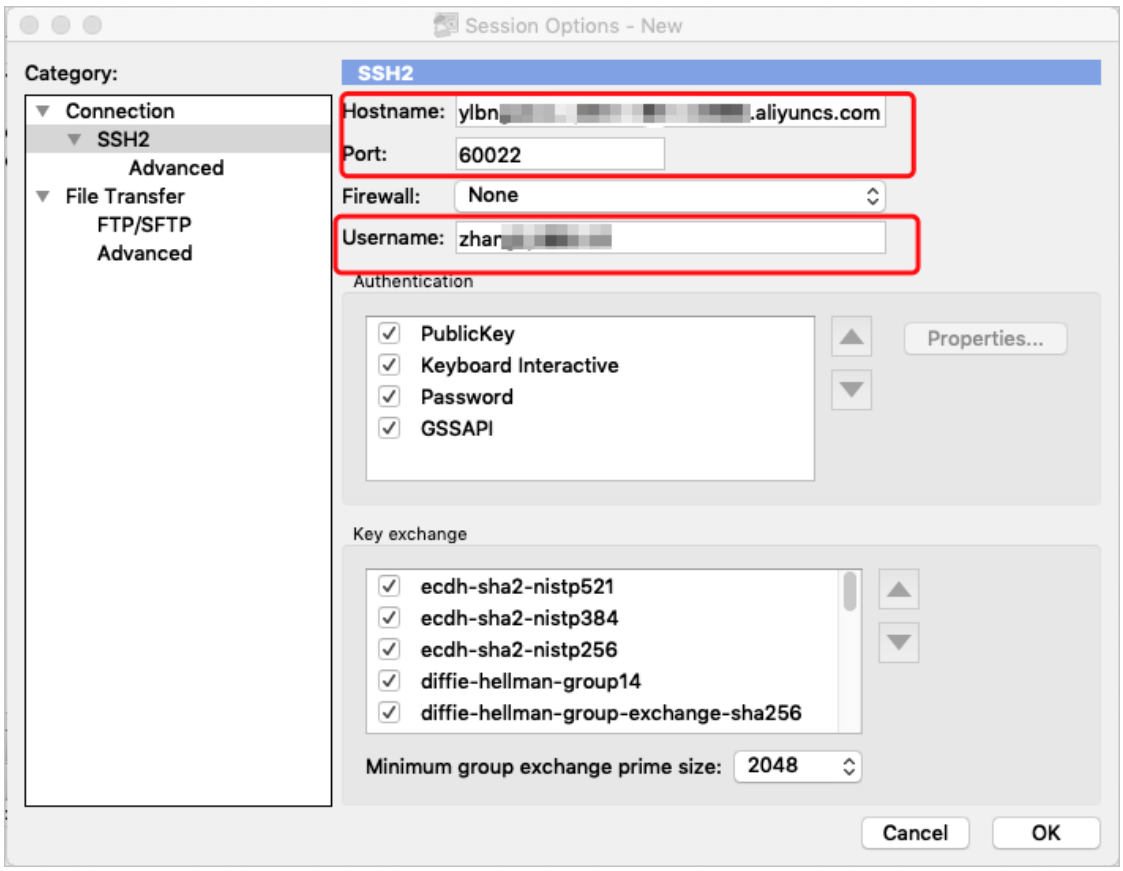
Procedure

1. Start the SecureFX tool.

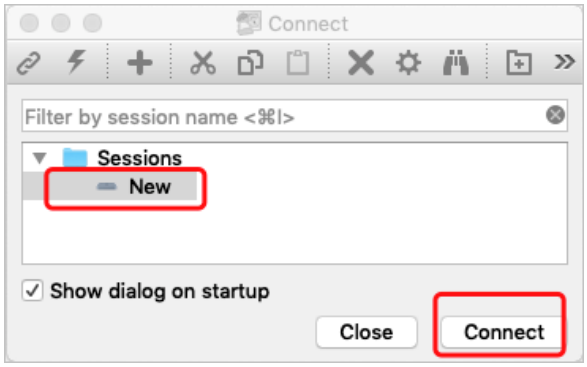
2. Click **Connect** in the upper-left corner. In the Connect dialog box, click the + icon.



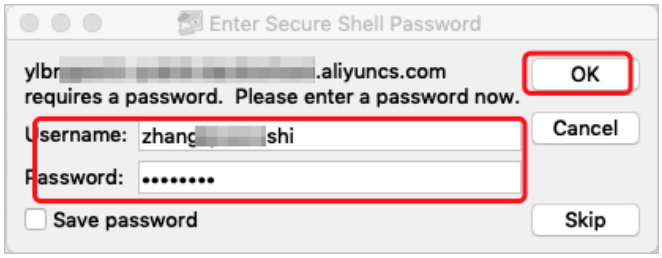
3. In the Session Options - New dialog box, enter the O&M portal of the bastion host in the Hostname field, the default port number 60022, and a username used to access the bastion host. Then, click **OK**.



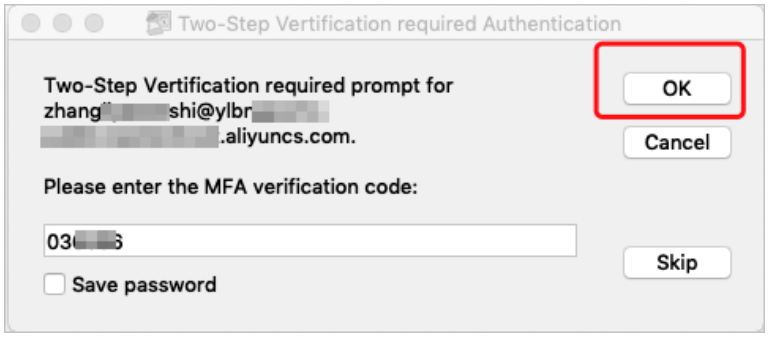
4. Select the created bastion host and click **Connect**.



5. In the Enter Secure Shell Password dialog box, enter the username and password of a RAM user and click **OK**.

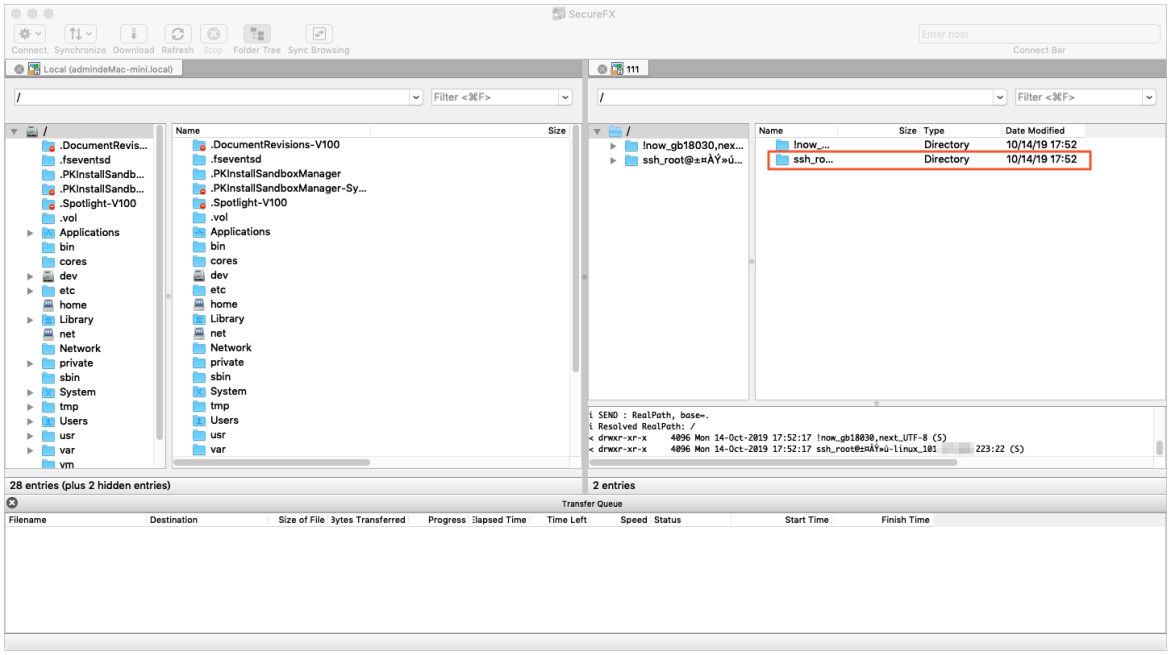


6. (Optional)If multi-factor authentication (MFA) is enabled for a RAM user, enter the verification code that you obtained from the bound MFA device (the Alibaba Cloud app) in the two-step verification dialog box and click **OK**.



7. After you log on to the bastion host, double-click the host for which you want to perform O&M operations to access the host directory and transfer files.

> **Note** If you cannot access the host directory, use one of the following methods to resolve the issue:
>
> - Check whether the username and password of the host are managed in Bastionhost. If the username and password of the host are not configured in Bastionhost, configure the username and password of the host. For more information, see Create an account for a host.
> - Check whether the name of the host directory is garbled. If the name of the host directory is garbled, you can double-click a transcoding directory and ignore the error message. Then, you can right-click the blank space and select Refresh to transcode the garbled directory name.
> - Clear the cache on SecureFX.
>
> If none of the preceding methods resolve your issue, submit a .


SecureFX
Connect
Synchronize
Download
Refresh
Stop
Folder Tree
Sync Browsing
Enter host
Connect Bar
Local (admindeMac-mini.local)
111
Filter <⌘F>
Name
Size
Type
Date Modified
.DocumentRevisions-V100
.fseventsd
.PKInstallSandboxManager
.Spotlight-V100
.vol
Applications
bin
cores
dev
etc
home
Library
net
Network
private
sbin
System
tmp
Users
usr
var
!now_gb18030,next_UTF-8 (S)
Directory
10/14/19 17:52
223:22 (S)
28 entries (plus 2 hidden entries)
2 entries
Transfer Queue
Filename
Destination
Size of File
Bytes Transferred
Progress
Elapsed Time
Time Left
Speed
Status
Start Time
Finish Time