ALIBABA CLOUD

Alibaba Cloud

Bastion Host

Quick Start

Document Version: 20220331

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.Overview

This topic describes how to deploy hosts, users, and O&M rules, implement O&M on hosts, and audit O&M sessions after you create a bastion host in Bastionhost V3.2.

The following table describes the steps.

Step	Description
Step 1: Synchronize ECS instances	The administrator adds the host to be managed to the bastion host. In this step, the administrator can synchronize the Elastic Compute Service (ECS) instances that belong to the current Alibaba Cloud account to the bastion host and create host accounts.
Step 2: Import Alibaba Cloud RAM users	The administrator adds users to the bastion host. In this step, the administrator can import Alibaba Cloud RAM users to the bastion host.
Step 3: Create O&M rules	The administrator creates O&M rules to authorize specific users to perform O&M operations on specific assets. In this step, the administrator creates O&M rules and authorizes specific users to perform O&M operations on specific hosts and host accounts.
Step 4: Perform O&M operations on hosts	Users (O&M personnel) access authorized hosts and perform O&M operations in client/server (C/S) O&M mode.
Step 5: Audit O&M sessions	When users log on to the bastion host in SSH, RDP, or SFTP mode to perform O&M operations on authorized hosts, the administrator can view the O&M session details in the console of the bastion host. In this step, the administrator can query and audit O&M operations and block high-risk sessions in the bastion host.

For more information about operations in Bastionhost, such as how to configure user groups or host groups at a time, see User Guide (V3.2).

2.Enable a bastion host

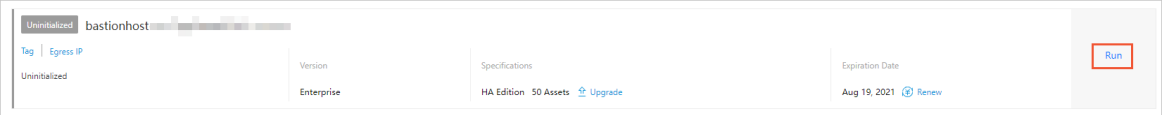
After you purchase a bastion host, you must enable the bastion host to use its features. This topic describes how to enable a bastion host.

Context

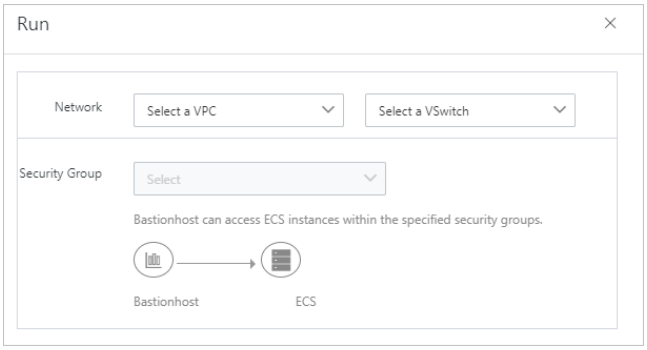
The newly purchased bastion host is uninitialized. You must enable the bastion host to use its features.

Procedure

1.
2. In the bastion host list, find the bastion host that you want to enable and click **Run**.



3. In the **Run** panel, configure the parameters.



The following table describes the parameters.

Parameter	Description

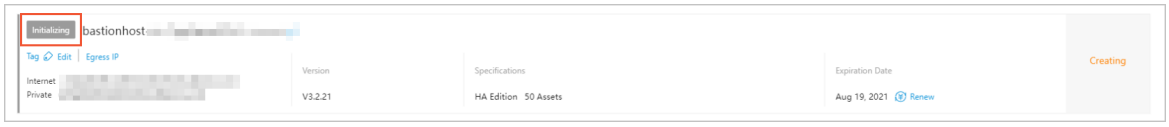
Parameter	Description
Network	Select a virtual private cloud (VPC) and vSwitch for the bastion host. **Notice** ◦ After the bastion host is enabled, you cannot change the VPC and vSwitch. ◦ To ensure that the bastion host can communicate with the Elastic Compute Service (ECS) instance that you want to maintain over an internal network, we recommend that you select the VPC in which the ECS instance resides. ◦ If the selected vSwitch does not have available resources, the bastion host fails to be enabled. If the bastion host fails to be enabled because the selected vSwitch cannot provide the required resources, select another vSwitch and enable the bastion host again. You can create a vSwitch to use before you enable the bastion host. For more information, see Create a vSwitch.

Parameter	Description
Security Group	Select the security group of the required ECS instances. **Note** - A bastion host must be added to at least one basic security group before the bastion host can be enabled. After the bastion host is enabled, you can modify security groups to which the bastion host belongs. After a bastion host is added to a basic security group, a security group rule is automatically generated to allow the bastion host to access all ECS instances in the security group. - You can also manually configure a security group rule for a bastion host. After you configure a security group rule for the bastion host, you do not need to add the bastion host to a security group. For more information, see Add security group rules. - You cannot add a bastion host to an advanced security group. You must manually configure a rule for an advanced security group to implement network communication. For more information, see Add security group rules.

4. Click **OK**.

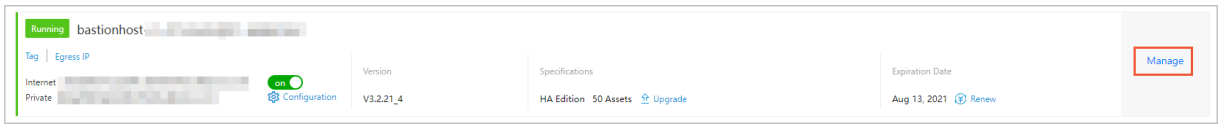
   The status of the bastion host changes to **Initializing**.

   Note It requires about 20 minutes for the bastion host to be initialized. Wait until the initialization is complete. After the initialization is complete, the status of the bastion host changes to **Running**. The bastion host is enabled.



Result

After the bastion host is enabled, you can click **Manage** to go to the console of the bastion host.



3.Log on to Bastionhost

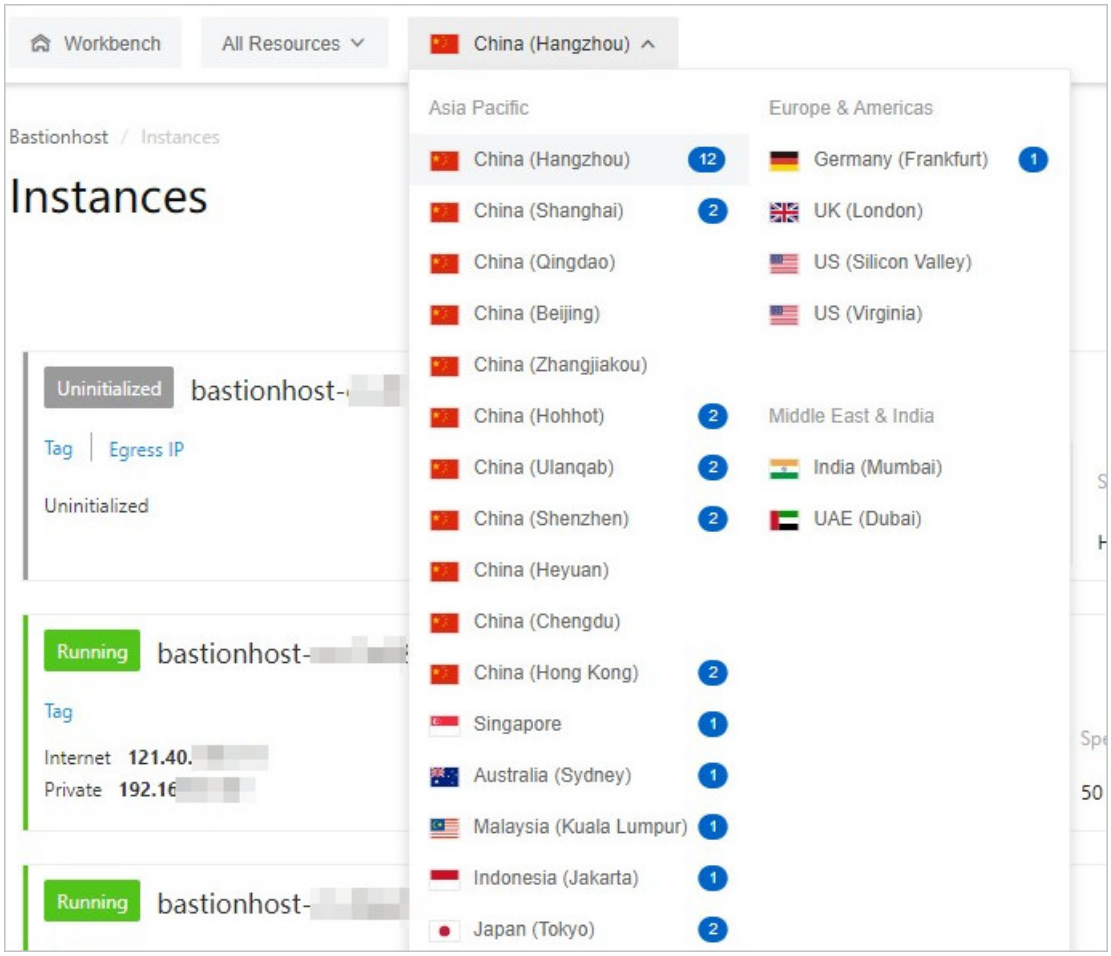
This topic describes how to log on to Bastionhost from a browser.

Context

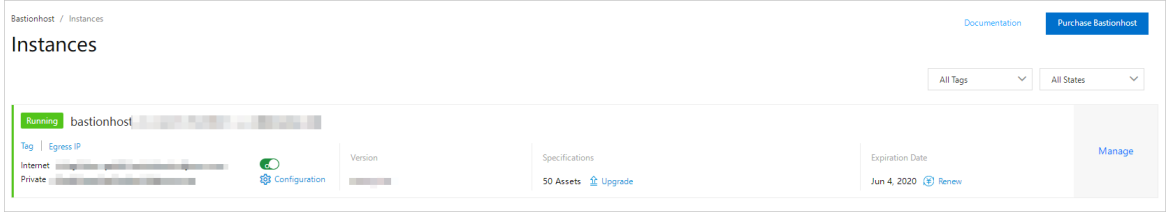
You can use an Alibaba Cloud account or a RAM user to log on to Bastionhost.

Procedure

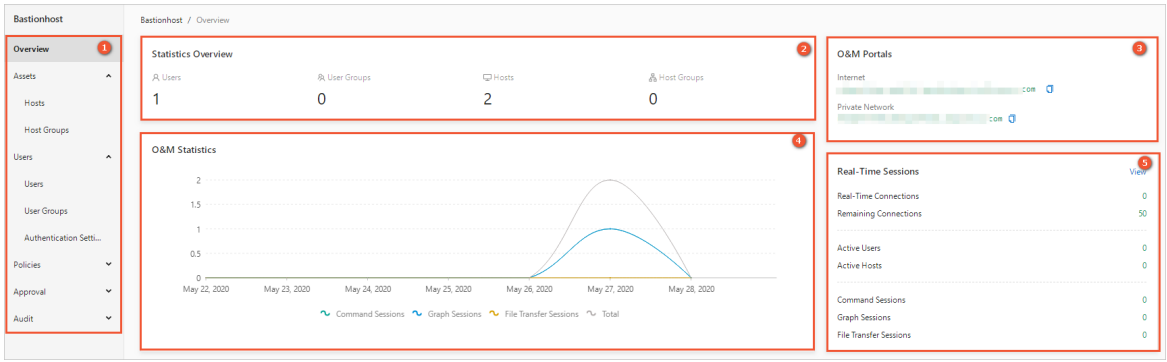
1.
2. In the top navigation bar, select the region where Bastionhost resides.



3. Find the Bastionhost instance you want to access and click **Manage**.



4. On the **Overview** page, perform O&M operations.



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

No.	Description
①	The menu items of Bastionhost.
②	The numbers of existing users, user groups, hosts, and host groups in Bastionhost.
③	The Internet and private network portals for users to perform O&M operations in Bastionhost.
④	The O&M statistics.
⑤	The information of real-time sessions.

4.Step 1: Synchronize ECS instances

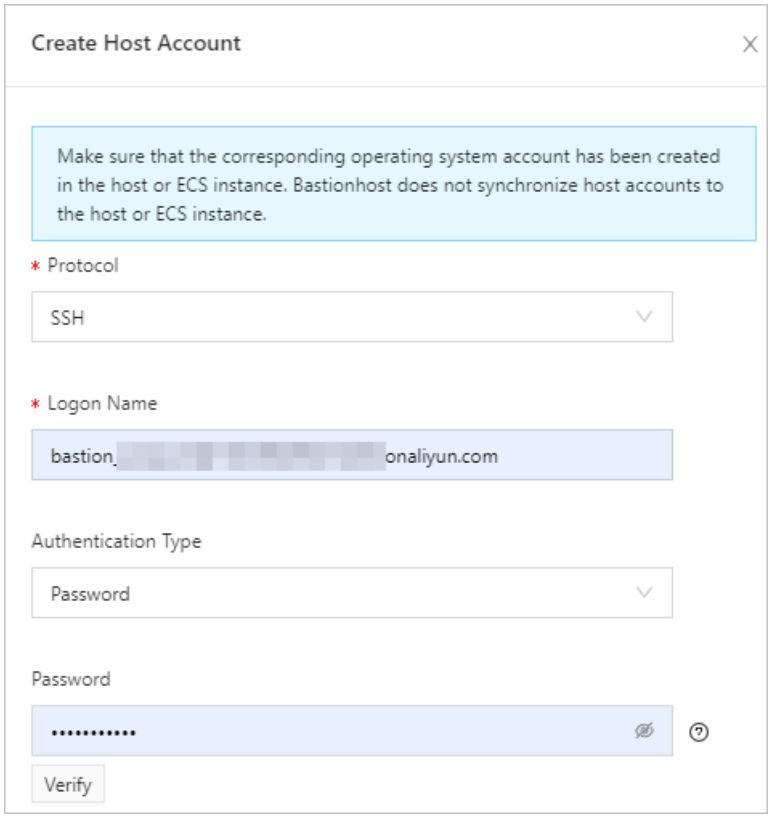
Before Bastionhost users can perform O&M operations on hosts, an administrator must add hosts to be managed to a bastion host and add accounts to the hosts. This topic describes how to import Elastic Compute Service (ECS) instances that belong to the current Alibaba Cloud account to a bastion host and add accounts to the hosts.

Context

You can also manually add hosts, import hosts by using a file, or import dedicated host groups of ApsaraDB RDS. For more information, see Import hosts from other sources.

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**.

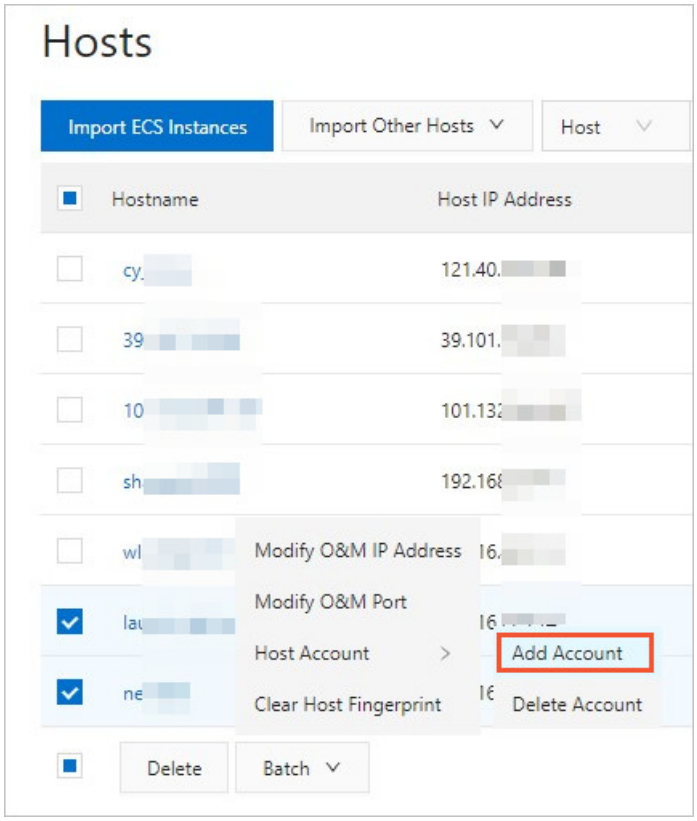


     c. Click **Verify**.

        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**.

5.Step 2: Import Alibaba Cloud RAM users

Before Bastionhost users can perform O&M operations on hosts, the administrator must create Bastionhost users in a Bastionhost instance. This topic describes how to import Alibaba Cloud RAM users to a Bastionhost instance as Bastionhost users.

Prerequisites

- RAM users are created under the Alibaba Cloud account for which the Bastionhost instance is created. For information about how to create RAM users, see Create a RAM user.
- RAM users to be imported are bound to virtual multi-factor authentication (MFA) devices if necessary. For information about how to bind a RAM user to a virtual MFA device, see Enable an MFA device for a RAM user.

Procedure

1.
2.
3.
4. In the Import RAM Users dialog box, select the RAM user that you want to import.

   > **Note** To import a single RAM user, click **Import** in the **Actions** column. In the message that appears, click Import.

5. Click **Import**.
   After the RAM user is imported, an O&M administrator can use the RAM user to log on to the bastion host.

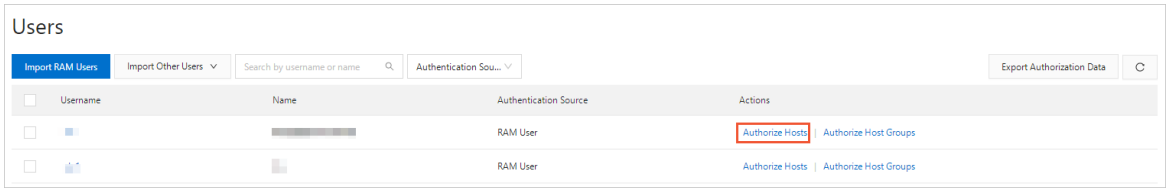
6.Step 3: Create O&M rules

Before Bastionhost users can perform O&M operations on hosts, the administrator must create O&M rules to authorize the users to perform O&M operations on specific hosts and host accounts. This topic describes how to create O&M rules.

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.

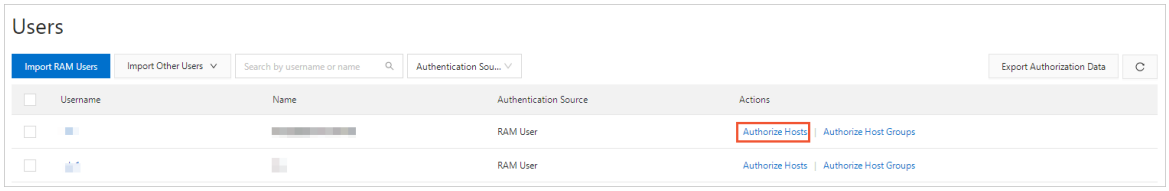


4. On the **Authorized Hosts** tab, click **Authorize Hosts**.
5. In the Authorize Hosts panel, select one or more hosts you want to authorize the user to manage and click **OK**.

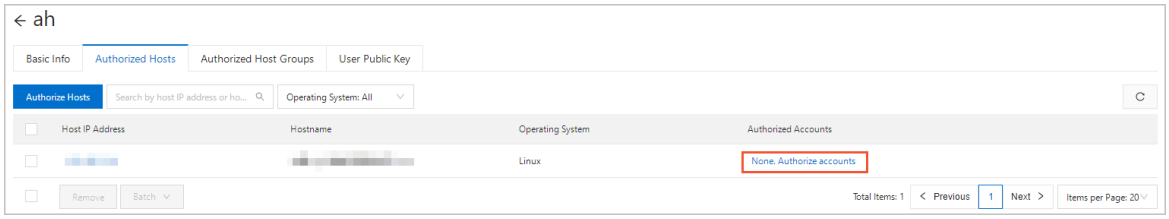
Authorize the accounts of a single host for a user

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.



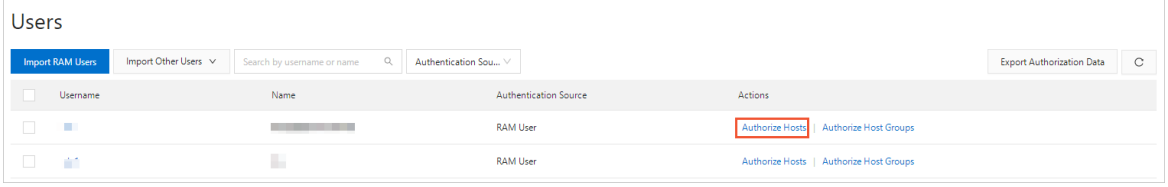
5. In the Select Accounts panel, select one or more accounts and click **Update**.

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

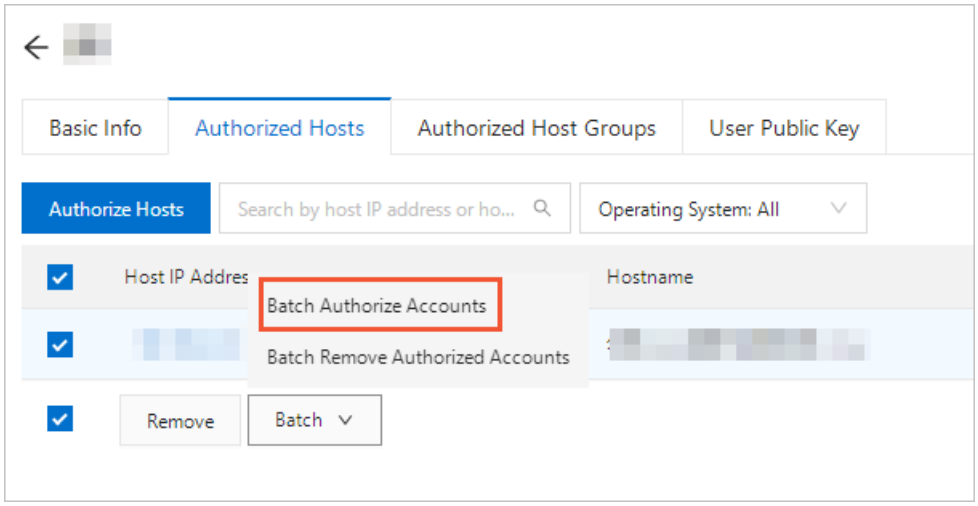
Authorize the accounts of multiple hosts for a user

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

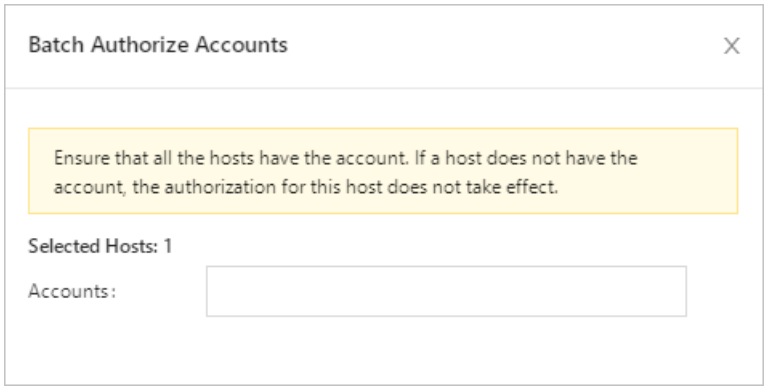
1.
2.
3. Find the user whom you want to authorize to manage hosts and click **Authorize Hosts** in the **Actions** column.



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**.

7.Step 4: Perform O&M operations on hosts

After the administrator has deployed host assets, Bastionhost users, and O&M rules in a Bastionhost instance, the Bastionhost users can access authorized hosts and perform O&M operations in client-server (CS) O&M mode. This topic describes how to configure O&M information and log on to the target server to perform O&M operations in CS O&M mode.

CS O&M refers to the process where Bastionhost users use a local client tool to log on to Bastionhost, access the target server, and perform O&M operations. Windows and macOS operating systems are supported.

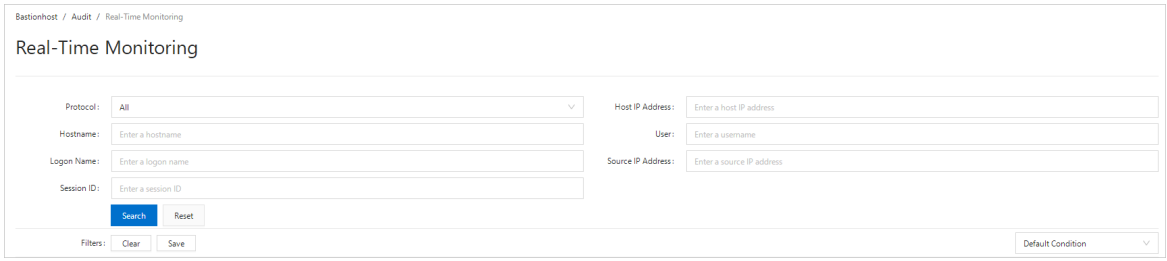
- Windows:
  - SSH-based O&M
  - RDP-based O&M
  - SFTP-based O&M
- macOS:
  - SSH-based O&M
  - RDP-based O&M
  - SFTP-based O&M

8.Step 5: Audit O&M sessions

When Bastionhost users log on to Bastionhost in SSH, RDP, or SFTP mode and perform O&M operations on authorized hosts, the administrator can view the O&M session details on the management page of the Bastionhost console. This topic describes how to query and audit O&M operations and interrupt high-risk sessions in a Bastionhost instance.

Search for sessions

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



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

Search condition	Description
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.

4. (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.

5. Click **Search**.