# Alibaba Cloud

Bastion Host User Guide (V3.2)

Document Version: 20220707

C-J 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.

- You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloudauthorized 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 and/or its affiliates 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		
A 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.		
O 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.		
C) 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.		
		Click Settings> Network> Set network type.		
>	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 Settings> Network> Set network type. Click OK.		
> Bold Courier font	Closing angle brackets are used to indicate a multi-level menu cascade. Bold formatting is used for buttons , menus, page names, and other UI elements. Courier font is used for commands	Click Settings> Network> Set network type. Click OK. Run the cd /d C:/window command to enter the Windows system folder.		
> Bold Courier font Italic	Closing angle brackets are used to indicate a multi-level menu cascade. Bold formatting is used for buttons , menus, page names, and other UI elements. Courier font is used for commands Italic formatting is used for parameters and variables.	Click Settings> Network> Set network type. Click OK. Run the cd /d C:/window command to enter the Windows system folder. bae log listinstanceid <i>Instance_ID</i>		
> Bold Courier font Italic [] or [a b]	Closing angle brackets are used to indicate a multi-level menu cascade. Bold formatting is used for buttons , menus, page names, and other UI elements. Courier font is used for commands Italic formatting is used for parameters and variables. This format is used for an optional value, where only one item can be selected.	Click Settings> Network> Set network type. Click OK. Run the cd /d C:/window command to enter the Windows system folder. bae log listinstanceid <i>Instance_ID</i> ipconfig [-all -t]		

# Table of Contents

1.Administrator manual	07
1.1. Authorize Bastionhost to access cloud resources	07
1.2. Log on to a bastion host	09
1.3. Instances	11
1.3.1. Configure a bastion host	11
1.3.2. Manage tags of Bastionhost instances	14
1.4. Asset management	15
1.4.1. Host management	15
1.4.1.1. Add hosts	15
1.4.1.2. Manage a host	17
1.4.1.3. Change the service port of a host	20
1.4.1.4. Create an account for a host	21
1.4.1.5. Configure account information for a host	22
1.4.1.6. Change the O&M IP address of a host	26
1.4.1.7. Clear host fingerprints	27
1.4.1.8. Export the host list with a few clicks	28
1.4.2. Manage asset groups	28
1.4.3. Use the automatic password change feature	29
1.4.4. Use the key management feature	33
1.4.5. Use the network domain feature	35
1.5. Manage users	38
1.5.1. User management	38
1.5.1.1. Manage users	38
1.5.1.2. Modify user information	43
1.5.1.3. Lock or unlock a user	44
1.5.1.4. Host the public key of a user	45

1.5.1.5. Delete users	46
1.5.2. User group management	47
1.5.2.1. Create a user group	47
1.5.2.2. Modify the information of a user group and delete	48
1.5.2.3. Add or remove users to or from a user group	48
1.5.3. Host authorization	50
1.5.3.1. Authorize a user to manage hosts	50
1.5.3.2. Authorize a user group to manage hosts	53
1.5.3.3. Export authorization data	56
1.5.4. Host group authorization	57
1.5.4.1. Authorize a user to manage host groups	57
1.5.4.2. Authorize a user group to manage host groups	61
1.6. Authorization rules	65
1.6.1. Create an authorization rule	65
1.6.2. Manage an authorization rule	67
1.7. policies	68
1.7.1. Create a control policy	68
1.7.2. Manage control policies	71
1.8. Approval	74
1.8.1. Approve commands	74
1.9. Auditing	75
1.9.1. Session audit	75
1.9.1.1. Search for sessions and view session details	75
1.9.1.2. Archive audit logs in Log Service	78
1.9.1.3. Use the log backup feature	80
1.9.2. Real-time monitoring	80
1.9.2.1. Search for real-time monitoring sessions and view s	80
1.9.2.2. Interrupt sessions	82

	1.9.3. Operations logs	82
	1.9.3.1. Search for operation logs and view log details	82
	1.9.4. O&M reports	83
1	.10. O&M	85
	1.10.1. Use the host O&M feature	86
1	.11. System settings	87
	1.11.1. Configure the parameters on the User Settings tab	87
	1.11.2. Enable two-factor authentication	88
	1.11.3. Configure AD authentication	90
	1.11.4. Configure LDAP authentication	91
	1.11.5. Diagnose network issues	92
	1.11.6. Configure O&M settings	93
	1.11.7. Use the storage management feature	96
	1.11.8. Use the notification feature	97
	1.11.9. Use the configuration backup feature	99
	1.11.10. Manage third-party asset sources	101
2.0	0&M manual	103
2	2.1. O&M overview	103
2	2.2. Windows client-based O&M	103
	2.2.1. SSH-based O&M	103
	2.2.2. RDP-based O&M	107
	2.2.3. Perform SFTP-based O&M	110
2	2.3. macOS client-based O&M	113
	2.3.1. SSH-based O&M	114
	2.3.2. RDP-based O&M	115
	2.3.3. Perform SFTP-based O&M	117

# **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

Onte 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"
                    1
                }
            }
       }
   ],
    "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.

All Resources	China (Hangzhou) ^	
	Asia Pacific Eu	rope & Americas
astionhost / Instances	China (Hangzhou) 🚺 📒	Germany (Frankfurt)
nstances	China (Shanghai) (2)	UK (London)
	China (Qingdao)	US (Silicon Valley)
	China (Beijing)	US (Virginia)
	China (Zhangjiakou)	
Dastionnost-	China (Hohhot) (2) Mic	ddle East & India
Tag Egress IP	🞦 China (Ulanqab) 🔹 🔤	India (Mumbai)
Uninitialized	China (Shenzhen) 🔹 📘	UAE (Dubai)
	China (Heyuan)	r
	China (Chengdu)	
Running bastionhost-	China (Hong Kong) 🛛 🕘	
Tag	Singapore 🚺	Sp
Internet 121.40. Private 192.16	🌇 Australia (Sydney) 🚺	50
	🖳 Malaysia (Kuala Lumpur) 1	50
	💻 Indonesia (Jakarta) 🛛 🕚	
bastionhost-	Japan (Tokyo)     2	

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

Bastionhost / Instances Instances				Documenta	tion	Purcha	ase Bastionhost
				All Tags	~	All States	s v
Running bastionhost							
Tag   Egress IP Internet C Private (@ Configu	Version	Specifications 50 Assets 🔮 Upgrade	Expiration Date	e ④ Renew			Manage

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

Bastionhost	Bastionhost / Overview	
Overview 1	Statistics Overview	O&M Portals
Assets •	A Users & User Groups C Horts & & Hort Groups 1 0 2 0	Internet con () Private Network con ()
Users ^	O&M Statistics	Real-Time Sessions
Users User Groups		Real-Time Connections 0 Remaining Connections 50
Authentication Setti Policies 🗸		Active Users 0 Active Hosts 0
Approval V Audit V	May 22, 2020 May 23, 2020 May 24, 2020 May 25, 2020 May 25, 2020 May 27, 2020 May 28, 2020	Command Sessions 0 Graph Sessions 0 File Transfer Sessions 0

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.

Create Host	Create User	O&M Authorization	Host O&M	Operation Manual
- - -	8	Å	品	-
Import ECS Instances Import assets with one click. Create Host Add a single host. Import Hosts from File You can import multiple hosts from an XLS, CSV, or XLSX file at a time.	Import RAM Users MFA is enabled for two-factor authentication of RAM users. Add Local User SMS verification codes are used for two-factor authentication of local users. Import Users from File You can import multiple local users	Authorization by User Grant permissions on host access to users and assign the credentials available for host access to users.	Bastionhost O&M Port SSH: 60022 RDP: 63389 Internet Portal for O&M of Local Clients rydhqircxj-public.bastionhosta Private Network Portal for O&M of Local Clients rydhqircxj.bastionhostaliyuncs	Operator Manual Administrator Manual

# 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.

- 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.

Network Sett	ings	×
Network	vpc-bp vsw-bp	
Security Group	sq-bp1fzs       Bastionhost can access ECS instances within the specified security groups.       Image: Control of the specified security groups.       Bastionhost     ECS	
Note: Security Gr	oup cannot be empty.	

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.

Network	1 vpc-bp
	🚯 vsw-bp
Public IP Address Whitelist	Enter a maximum of 30 IP addresses. Separate them with commas (,).

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**.

1 vpc-bp			
1 vsw-bp			
	Custom	60021	Modify ③
	Custom	60022	Modify ③
	Custom	60023	Modify ③
63389	Custom	63389	Modify ③
61022	Custom	61022	Modify ③
	<ul> <li>vpc-bp</li> <li>vsw-bp</li> <li>60021</li> <li>60022</li> <li>60023</li> <li>63389</li> <li>61022</li> </ul>	vpc-bp     vsw-bp      60021     Custom      60022     Custom      60023     Custom      63389     Custom      61022     Custom	<ul> <li>▲ vpc-bp</li> <li>▲ vsw-bp</li> <li>60021</li> <li>Custom</li> <li>60022</li> <li>Custom</li> <li>60023</li> <li>Custom</li> <li>60023</li> <li>63389</li> <li>Custom</li> <li>63389</li> <li>Gasae</li> <li>61022</li> <li>Custom</li> <li>61022</li> </ul>

**?** 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.

g			:
Tag	No data.		
Add Tag		>	
		>	
		>	
Create Tag	Key	Value	OK Clea
			1

• Add tags

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

Onte 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.

Tag			×
	Tag	(key1: 2 🗙)	

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.

	Documentation			Purchase B	astionhost
C	Select		^	All States	$\sim$
	All Tags		2		
	1	>			
te		.>			Manage
6	key1	>			
ĸ	key2	>			

# 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.

ONOTE 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 Host name 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.

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.

- 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.

<sup>1.</sup> 

- 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.

Hosts								
Import ECS Instances	Import Other Hosts 🗸 🛛 Host 🗸	Search by hostname or h Q	Operating System: All	V Host Source: All	$\vee$ Host Status: All $\vee$			Export Hosts C
Hostname	Host IP Address	Remarks	Host Accounts	Network Domain	Operating System	Host Source	Host Status	Actions
Q.J	192.168		0	Direct Network	Linux	ECS	Normal	Create Host Account   Delete
39.10	39.101		1	Direct Network	Windows	Local	Normal	Create Host Account   Delete
101.132.	101.132		1	Direct Network	Linux	Local	Normal	Create Host Account   Delete
shangh	192.168		1	shanghaicy	Linux	Local	Normal	Create Host Account   Delete
w	172.16		0	Direct Network	Linux	ECS	Normal	Create Host Account   Delete

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

- Search by host name 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.

- 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.

Basic Info	Service Port	Host Account	
<ul> <li>Operating Syste</li> </ul>	m		
Windows			$\sim$
<ul> <li>Host IP Address</li> </ul>			
39.101.			
Hostname			
39.101			
Network Domain			
Direct Network	(Direct Connection	1)	$\sim$
Remarks			
Host Group			
Update			

(?) Note You cannot modify the Host IP Address or Host name 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.

- 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 host name.
- 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.

	Hostname	Host IP Address	Remarks	Host Accounts	Operating System	Host Source	Actions
				0	Linux	Local	Delete
	Modify O&M IP Address			0	Linux	ECS	Delete
<	Create Account for Hosts	0.000		0	Windows	ECS	Delete
	Delete Batch V				Total Items: 3	C Previous 1 Next >	Items per Page: 20 $\vee$

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

Modify O&N	Port		×
Protocol :	SSH	~	
Port:	22		
		ОК	Cancel

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.

- 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**.

Create Host Account	Х
Make sure that the corresponding operating system account has been cr in the host or ECS instance. Bastionhost does not synchronize host accou the host or ECS instance.	eated ints to
* Protocol SSH V	
* Logon Name	
Authentication Type	
Password V	
/ Verifiz	0
veny	

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**.

Hosts	
Import ECS Instances	Import Other Hosts V Host V
Hostname	Host IP Address
cy.	121.40.
39	39.101.
10	101.132
sh	192.16
wl	Modify O&M IP Address 16.
✓ lau	Modify O&M Port Host Account > Add Account
🖌 ne	Clear Host Fingerprint <sup>16</sup> Delete Account
Delete	Batch 🗸

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 host name.
- 4. In the pane that appears, click the **Host Account** tab.

Basic I	nfo Servic	e Port	Host Accoun	it			
Create	Host Account	Searc	h by logon name	Q			
	Logon Name		Protocol	Password		SSH Private Key	
			SSH	Available	Clear	None Set	
	Delete			<	1 /	1 ) Items ner F	Page: 20

- 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.

Edit Host Account		×
* Logon Name		
Password	ø	0
Verify		
Save		

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.

- 3. On the **Hosts** page, find the target host and click the host name.
- 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.

						>
Basic I	nfo Service	Port Host Accou	nt			
Create	Host Account	Search by logon name	Q			С
	Logon Name	Protocol	Password		SSH Private Key	
		SSH	Available	Clear	None Set	
<b>~</b>	÷.	SSH	Available	Clear	None Set	
	Delete		<	1	1 > Items per Pag	e: 20 ∨

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

Are you sure you want to delete the selected accounts?
 Cancel 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 host name.
- 4. In the pane that appears, click the **Host Account** tab.

				:
Basic Info	Service Port	Host Account		
Create Host A	Account Searc	h by logon name	Q	C
Logo	n Name	Protocol	Password	SSH Private Key
		SSH	Available Clear	None Set
De	lete		< 1	/ 1 > Items per Page: 20 V

- 5. On the Host Account tab, set, change, or delete a password.
  - $\circ~$  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 host name.
- 4. In the pane that appears, click the Host Account tab.

Basic I	nfo Service	e Port	Host Account	t	
Create	Host Account	Searc	h by logon name	Q	
	Logon Name		Protocol	Password	SSH Private Key
	1000		SSH	Available Clear	None Set

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

Basic Info	Service	e Port	Host Accour	it			
Create Hos	st Account	Search	by logon name	Q			С
Lo	ogon Name		Protocol	Password		SSH Private Key	
			SSH	Available	Clear	None Set	
			SSH	Available	Clear	None Set	
	Delete			<	1	1 > Items per Page	e: 20 V

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

#### ? Note

• Bastionhost supports only Rivest-Shamir-Adleman (RSA) private keys generated by **sshkeygen**.

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.

Set Private Key	Х
Only an RSA private key generated by ssh-keygen is supported.	
* Private Key :	
	h
Encrypted Password : 🖾 🖉 🕥	
	Save Cancel

- 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.

Hostname	Host IP Address	Remarks	Host Accounts	Operating System	Host Source	Actions
			0	Linux	Local	Delete
Modify O&M IP Address			0	Linux	ECS	Delete
Create Account for Hosts	0.000		0	Windows	ECS	Delete
Delete Batch V				Total Items: 3	< Previous 1 Next >	Items per Page: 20 ∨

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

Modify O&M IP Addre	55		X
Host IP Address Type :	Private IP Address	$\vee$	
		ОК	Cancel

- 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.

Basic Info	Service Port	Host Account			
You cannot mo	odify the host inform	ation of an ECS instar	ce or a dedicated cluster.		
Operating Syste	m				
				$\sim$	
Host IP Address					
ostname					
emarks					
				0	0
ost Fingerprint					
o host fingerpri	clear				
o nosc nigerpri					
ost Group					

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.

<b>Z</b>	Modify O&M IP Address	192.1	2	Linux
	Modify O&M Port	118.1	2	Windows
<b>v</b>	Host Account > Clear Host Fingerprint	192.1	2	Linux
Dele	te Batch ∨			

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.

Hosts										
Import ECS Instances	Import Other Hosts 🗸	Host $\vee$	Search by hostname or h Q	Operating System: All	✓ Host Source: All ✓	Host Status: All $\qquad \lor$			Export Hosts	С
Hostname	Host IP	Address	Remarks	Host Accounts	Operating System	Host Source	Host Status	Actions		
				1	Windows	ECS	<ul> <li>Normal</li> </ul>	Create Host Acco	ount   Delete	
				1	Linux	ECS	<ul> <li>Normal</li> </ul>	Create Host Acco	ount   Delete	

# 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.

OS	Version
Alibaba Cloud Linux	<ul> <li>3.2104 64-bit</li> <li>2.1903 LTS 64-bit</li> <li>2.1903 64-bit (Quick Start)</li> </ul>
CentOS	All versions
Ubuntu	All versions
Debian	All versions
Open SUSE	<ul> <li>15.1 64-bit</li> <li>15.2 64-bit</li> <li>42.3 64-bit</li> <li>7 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.</li> </ul>
SUSE Linux	<ul> <li>SUSE Linux Enterprise Server 15 SP2 64-bit</li> <li>SUSE Linux Enterprise Server 12 SP5 64-bit</li> <li>SUSE Linux Enterprise Server 11 SP4 64-bit</li> </ul>
CoreOS	<ul> <li>2303.4.0 64-bit</li> <li>2247.6.0 64-bit</li> <li>2023.4.0 64-bit</li> <li>1745.7.0 64-bit</li> </ul>

#### Supported OSs and versions

#### Create a password change task

- 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	<ul> <li>The execution method of the password change task. Valid values:</li> <li>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.</li> <li>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.</li> </ul>
Password Rules	<ul> <li>The complexity and length settings of the new password.</li> <li>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.</li> <li>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.</li> </ul>
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.

text1					Х
Task Details	Managed Accounts				
Add Host Accour	Search by host accou	int name 🔍			C
Host	Account N	ame Protoc	ol Operating System	Status	Last Execution Ti

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**.

Onte 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.

Export Password	×
Enter a password to encrypt and compress a result file in the ZIP format. The length.	password must be 4 to 32 characters in
* Encrypt File:	ø
	Export Password Cancel

# 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.

Onte 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.

			×
* Proxy Type:	SSH Proxy	$\sim$	0
			~
* Server Address :			0
* Server Port:			
* Host Account:	bastio		
n Deservered -		a.	
* Password :		yes	
Test Connection			
	ОК	Ca	ancel

Parameter	Description	
Ргоху Туре	<ul> <li>The type of the proxy. Valid values:</li> <li>SSH Proxy</li> <li>HTTP Proxy</li> <li>SOCKS5 Proxy</li> </ul>	
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. ClickTest 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.
- Maint ain 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 <b>Username</b> , <b>Password</b> , <b>User Group</b> , and <b>Remarks</b> . You can also perform the following operations:
	<ul> <li>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.</li> </ul>
	<ul> <li>This parameter is valid only for local users.</li> <li>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&amp;M administrator cannot use the local user to log on to the bastion host.</li> </ul>

Scenario	<ul> <li>Configure Two-factor Authentication Methods: If you enable Two- Procedure Tactor Authentication Methods, the local user must enter a dynamic</li> </ul>		
	verification code that is sent by text message, email, or DingTalk after the local user enters the valid password. This helps reduce security risks.		
Create a single local user	<ul> <li>Note</li> <li>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.</li> <li>The mobile phone number and email address that you entered are used only to receive verification codes or alert notifications.</li> </ul>		
	Valid values of <b>Two-factor Authentication Methods</b> :		
	<ul> <li>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.</li> </ul>		
	<ul> <li>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:</li> </ul>		
	Disable: specifies that two-factor authentication is disabled.		
	<ul> <li>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.</li> </ul>		
	<ul> <li>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.</li> </ul>		
	<ul> <li>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.</li> </ul>		
	<b>Note</b> 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	<ul> <li>i. Select Import Users from File from the Import Other Users drop-down list.</li> <li>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.</li> <li>iii. In the Import Local Users dialog box, click Upload to upload the user template file that you edited.</li> <li>iv. In the Preview dialog box, select the local users that you want to import and click Import.</li> <li>v. In the Import Local Users panel, confirm the information about the local users.</li> <li>if you select Users must reset the password at next logon, all imported local users must reset their passwords upon the next logon.</li> <li>vi. Click Import Local Users.</li> </ul>
	(?) 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 <b>Details</b> in the <b>Import Local Users</b> 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 LDAPauthenticated 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

> Document Version: 20220707

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.

Votice 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.

Bastionhost / U	sers / Users / User Deta	ils				
< opera	← operator					
Basic Info	Authorized Hosts	Authorized Host Groups	User Public Key	,		
* Username						
operator						
* Name						
- Name				0		
Password						
			e se	0		
Mobile Number						
+86 🗸	+86 ∨					
Update						

**?** 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.

Add SSH Public Key	
* Public Key Name:	
	0
* Public Key:	
Remarks :	
	0
Parameter	Description

l'alameter	beschption
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.

Users					
Impor	t RAM Users Import Other Users V	Search by username or name Q	Authentication Sou $\vee$	Export Authorizatio	on Data C
	Username	Name	Authentication Source	Actions	
	-		RAM User	Authorize Hosts   Authorize Host Groups	
			RAM User	Authorize Hosts   Authorize Host Groups	
	- and the second s		Local Authentication	Authorize Hosts   Authorize Host Groups	
<b>~</b>			Local Authentication	Authorize Hosts   Authorize Host Groups	
<b>~</b>	Sec.	100	Local Authentication	Authorize Hosts   Authorize Host Groups	
	Unlock Delete			Total Items: 37         <         Previous         1         2         3         ···         8         Next >         It	tems per Page: 5 🗸

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.
- ۷.
- 3.
- 4. In the Create User Group pane, enter a user group name in the User Group Name field.

Create User Group	×
* User Group Name	0
Create User Group	

**?** 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.

User Groups				
Create User Group Search by user group name Q		С		
Name	Members	Actions		
Operation Group	2	Authorize Hosts   Authorize Host Groups		
Test Group	0	Authorize Hosts   Authorize Host Groups		
Delete		Total Items: 2 ≤ Previous 1 Next > Items per Page: 20 ∨		

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

Bastionhost / User / User Groups / User Group Details				
- Oper	ration G	roup		
Settings Members Authorized Hosts Authorized Host Groups				
User Group Na	ame			
Operation Group				0

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**.

User Groups				
Create	User Group Search by user group name Q,		С	
	Name	Members	Actions	
	Operation Group	2	Authorize Hosts   Authorize Host Groups	
	Test Group	0	Authorize Hosts   Authorize Host Groups	
	Delete		Total Items: 2 < Previous 1 Next > Items per Page: 20 V	

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.

User Groups		
Create User Group Search by user group name Q.		С
Name	Members	Actions
Operation Group	2	Authorize Hosts   Authorize Host Groups
Test Group	0	Authorize Hosts   Authorize Host Groups
Delete		Total Items: 2 < Previous 1 Next > Items per Page: 20 ∨

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

< Ope	ration G	iroup		
Settings	Members	Authorized Hosts	Authorized Host Groups	
Add Membe	r Search by	username or name O	×	
Use	ername		Name	
			1.00	

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

Add Member		х
Search by username or name Q		C
Username	Name	Actions
		Add
		Add
	1	Add
	1000	Add
	-	Add
Add		Total Items: 35         <

**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.

User Groups		
Create User Group Search by user group name Q		С
Name	Members	Actions
Operation Group	2	Authorize Hosts   Authorize Host Groups
Test Group	0	Authorize Hosts   Authorize Host Groups
Delete		Total Items: 2 < Previous 1 Next > Items per Page: 20 ∨

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

← Operation Group		
Settings Members Authorized Hosts Au	thorized Host Groups	
Add Member Search by username or name Q		С
✓ Username	Name	Actions
	1000	Remove
		Remove
Remove		Total Items: 2 < Previous 1 Next > Items per Page: 20 V

**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.

User	S								
Import	RAM Users	Import Other Users 🗸	Search by username or name	Authentication Sou V				Export Authorization Data	С
	Username		Name	Auth	entication Source	Actions			
				RAM	User	Authorize Hosts	Authorize Host Groups		
	11		10 C	RAM	User	Authorize Hosts	Authorize Host Groups		

- 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.

User	rs								
Import	RAM Users	Import Other Users V Search by use	mame or name Q	Authentication Sou $\vee$				Export Authorization Data	С
	Username	Name		Authe	ntication Source	Actions			
				RAM I	Jser	Authorize Hosts	Authorize Host Groups		
	11			RAMI	Jser	Authorize Hosts	Authorize Host Groups		

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

<			
Basic Info Authorized Hosts Authorized	Host Groups User Public Key		
Authorize Hosts Search by host IP address or ho	Q. Operating System: All ∨		С
Host IP Address	Hostname	Operating System	Authorized Accounts
		Linux	None. Authorize accounts
		Linux	None. Authorize accounts
Remove Batch V			Total Items: 2 < Prøvious 1 Next > Items per Page: 20 ∨

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.

Use	ers					
Impo	rt RAM Users	Import Other Users V Search by username or name Q	Authentication Sou $\vee$		Export Authorization Data	С
	Username	Name	Authentication Source	Actions		
			RAM User	Authorize Hosts   Authorize Host Groups		
	-		RAM User	Authorize Hosts   Authorize Host Groups		

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

<ul><li>← ah</li></ul>	1					
Basic	Info Authorized Hosts	Authorized Host Groups	User Public Key			
Author	ize Hosts Search by host IP	address or ho Q Operating	g System: All $\sim$			
	Host IP Address	Hostnam	1e	Operating System	Authorized Accounts	
		-		Linux	None. Authorize accounts	
	Remove Batch V				Total Items: 1 < Previous 1 Next > It	ems per P

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.

U	sers									
	mport RAM L	Users Im	port Other Users 🗸	Search by username or name	Q. Authentication Sou.	∨			Export Authorization Data	С
	Usen	mame		Name		Authentication Source	Actions			
						RAM User	Authorize Host	s   Authorize Host Groups		
		1		- N		RAM User	Authorize Host	s   Authorize Host Groups		

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

<					
Basic Info	Authorized Hosts	Authorized Host G	Groups	User Public Key	
Authorize Hos	Search by host IP	address or ho Q	Operating S	System: All 🛛 🗸	
✓ Host	IP Addres Batch Authoriz	ze Accounts	Hostname		
<b>~</b>	Batch Remove	Authorized Accounts			
✓ Re	emove Batch ∨				

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

Batch Authorize Accounts	×
Ensure that all the hosts have the account. If a host does not have the account, the authorization for this host does not take effect.	
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.

Users					
Import RAM Users	Import Other Users v Search by username or name Q	Authentication Sou $\vee$		Export Authorization Data	С
Username	Name	Authentication Source	Actions		
		RAM User	Authorize Hosts   Authorize Host Groups		
		RAM User	Authorize Hosts   Authorize Host Groups		

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

<b></b>	1.11						
Basic Inf	o Autł	horized Hosts	Authorized Hos	t Groups	User Public Key		
Authorize	Hosts	Search by host IP a	ddress or ho Q	Operating	g System: All 🛛 🗸 🗸		
✓ Host	IP Address			Hostn	ame		Operating System
✓ 19	6	Batch Authorize A	accounts	- 10			Linux
✓ 19	.7	Batch Remove Au	thorized Accounts				Windows
F	Remove	Batch 🗸					

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

< -			
Basic Info	Authorized Hosts	Authorized Host Groups	User Public Key
Authorize Hos	sts Search by host IP	address or ho Q Operating	g System: All 🛛 🗸
✓ Host	IP Addres Batch Authoriz	Hostnam	ne
	Batch Remove	Authorized Accounts	
✓ Re	emove Batch v		

**?** 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

<sup>&</sup>gt; Document Version: 20220707

1.

2.

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

User Groups		
Create User Group Search by user group name Q		С
Name	Members	Actions
Operation Group	1	Authorize Hosts   Authorize Host Groups
Test Group	0	Authorize Hosts   Authorize Host Groups
Delete		Total Items: 2 < Previous 1 Next > Items per Page: 20∨

- 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**.

<ul> <li>Host IP Address</li> <li>Hostname</li> <li>Operating System</li> <li>X</li> <li>Linux</li> <li>Windows</li> </ul>	
Linux     Windows	· x
Windows	

#### 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.

User Groups		
Create User Group Search by user group name Q.		С
Name	Members	Actions
Operation Group	1	Authorize Hosts   Authorize Host Groups
Test Group	0	Authorize Hosts   Authorize Host Groups
Delete		Total Items: 2 < Previous 1 Next > Items per Page: 20 ∨

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

< Ope	eration Grou	р						
Settings	Members Auth	horized Hosts	Authorized Host Groups					
Authorize	Hosts Search by host l	IP address or ho O	Operating System: All 🛛 🗸					С
	Host IP Address		Hostname	Ope	rating System	Authorized Accounts		
			the second second	Linu	х	None. Authorize accour	nts	
	Remove Batch ∨						Total Items: 1 < Previous 1 Next 2	Items per Page: 20 V

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.

User Groups		
Create User Group Search by user group name Q		C
Name	Members	Actions
Operation Group	1	Authorize Hosts   Authorize Host Groups
Test Group	0	Authorize Hosts   Authorize Host Groups
Delete		Total Items: 2 < Previous 1 Next > Items per Page: 20 ∨

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

← Operation Group			
Settings Members Authorized Hosts Authorized Host Groups			
Authorize Hosts Search by host IP address or ho Q Operating System: All V			С
Host IP Addres Hostname	Operating System	Authorized Accounts	
Batch Remove Authorized Accounts	Linux	None. Authorize accounts	
Remove Batch V		Total Items: 1 < Previous 1 Next >	Items per Page: 20 ∨

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

Batch Authorize Accounts	×
Ensure that all the hosts have the account. If a host does not have the account, the authorization for this host does not take effect. Selected Hosts: 1 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.

User Groups		
Create User Group Search by user group name Q		С
Name	Members	Actions
Operation Group	1	Authorize Hosts   Authorize Host Groups
Test Group	0	Authorize Hosts   Authorize Host Groups
Delete		Total Items: 2 < Previous 1 Next > Items per Page: 20 ∨

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

<ul> <li>← Operation Group</li> </ul>				
Settings Members Authorized Hosts Authorized	ed Host Groups			
Authorize Hosts Search by host IP address or ho Q Ope	rating System: All 🛛 🗸			С
Host IP Addres Hos	stname	Operating System	Authorized Accounts	
Batch Remove Authorized Accounts		Linux	None. Authorize accounts	
Remove Batch V			Total Items: 1 < Previous 1 Next > Ite	ems per Page: 20 ∨

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

Authorized Hosts	Authorized Host	Groups	User Public Key
Search by host IP a	address or ho Q	Operating S	System: All 🛛 🗸
ddres Batch Authorize	e Accounts	Hostname	:
Batch Remove	Authorized Accounts	-	
e Batch ∨			
	ldres Batch Authoriz Batch Remove e Batch ∨	ddres Batch Authorize Accounts Batch Remove Authorized Accounts e Batch V	ddres Batch Authorize Accounts Batch Remove Authorized Accounts e Batch ∨

**?** 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.

Bastionh	nost / Users / l	Jsers		
Use	rs			
Impo	rt RAM Users	Import Other Users V Search by username or name	Q Authentication Sou $\vee$	Export Authorization Data C
	Username	Name	Authentication Source	Actions
	-		RAM User	Authorize Hosts   Authorize Host Groups
		Delete		Total Items: 1 < Previous 1 Next > Items per Page: 20 ∨

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.

Bastionho	ost / Users / I	Jsers		
Use	rs			
Impor	t RAM Users	Import Other Users v Search by username or name	Q. Authentication Sou ∨	Export Authorization Data C
	Username	Name	Authentication Source	Actions
	-		RAM User	Authorize Hosts Authorize Host Groups
		Delete		Total Items: 1         <         Previous         1         Next         >         Items per Page: 20 ∨

- 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**.

∈ ah				
Basic Info	o Authorized Hosts	Authorized Host Groups U	ser Public Key	
Authorize	Host Groups Search by he	ost group name Q		
- F	Host Group Name		Authorized Accounts	
	test		root	
	Remove Batch V			Total Items: 1 < Previous 1 Next > Items: ner P

······

\_\_\_\_\_

#### 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**.

<				
Basic I	Info Authorized Hosts	Authorized Host Groups User Public Key	Key	
Author	rize Host Groups Search by host	group name Q		С
	Host Group Name	Authorized Acc	Accounts	
	test	root		
<b>Z</b>	Remove Batch V		Total Items: 1 < Previous 1 Next > Items per Page: 2	0~

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.

Bastionho	ost / Users / I	Jsers		
Use	rs			
Impor	rt RAM Users	Import Other Users V Search by username or name	Q. Authentication Sou V	Export Authorization Data C
	Username	Name	Authentication Source	Actions
			RAM User	Authorize Hosts Authorize Host Groups
		Delete		Total Items: 1 < Previous 1 Next > Items per Page: 20 \

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

÷			
Basic Info	Authorized Hosts	Authorized Host Groups	User Public Key
Authorize H	ost Groups Search by I	nost group name Q	
Но	st Group Name		Authorized Accounts
te	st		None. Authorize accounts
	Remove Batch ∨		

**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.

Select Accounts [test]					
Accounts:	Enter the accounts you want to authorize				
Update					

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.

Bastionho	ost / Users / l	Jsers		
User	rs			
Import	RAM Users	Import Other Users V Search by username or name	$\bigcirc$ Authentication Sou $\lor$	Export Authorization Data C
	Username	Name	Authentication Source	Actions
	-		RAM User	Authorize Hosts   Authorize Host Groups
		Delete		Total Items: 1 < Previous 1 Next > Items per Page: 20 V

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**.

Basic Info	Authorized Hosts	Authorized Host Groups	User Public Key
Authorize Hos	t Groups Search by h	ost group name Q	
<ul> <li>Host</li> </ul>	Group Name		Authorized Accounts
-	Batch Authoriz	e Accounts	None. Authorize accounts
			None Authorize accounts

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

Batch Authoriz	ze Accounts	×
Selected Host Gr	oups: 1	
Accounts:	Enter the accounts you want to authorize	
Update		

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.

1.05						
Basic Info	Authorized Hosts	Authorized Host Groups	User Public Key			
Authorize Host Groups     Search by host group name     Q						
✓ Host Group Name Authorized Accounts						
	Batch Authoriz	ze Accounts	root			
	Batch Remove	Authorized Accounts	root			
✓ Re	move Batch V					

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

Batch Remove Authorized Accounts				
Selected Host Gro	pups: 2			
Accounts:	Select or enter the authorized accounts you want			
Update				

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.

Bastionhost / Users / User Groups		
User Groups		
Create User Group Search by user group name Q		С
Name	Members	Actions
Operation Group	1	Authorize Hosts   Authorize Host Groups
Test Group	0	Authorize Hosts   Authorize Host Groups
Delete		Total Items: 2 < Previous 1 Next > Items per Page: 20 ∨

- 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**.

Authorize Host Groups			×
Search by host group name Q	< 1/1 >	Selected (2)	Clear
I ✓ Host Group Name		test	×
test		арі	×
api			
2			
ок			

#### 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.

Bastionhost / Users / User Groups		
User Groups		
Create User Group Search by user group name Q,		С
Name	Members	Actions
Operation Group	1	Authorize Hosts   Authorize Host Groups
Test Group	0	Authorize Hosts   Authorize Host Groups
Delete		Total Items: 2 < Previous 1 Next > Items per Page: 20∨

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

< Ope	ration G	roup									
Settings	Members	Authorized Hosts	Authorized Host Groups								
Authorize H	Host Groups	earch by host group name	Q.								С
He He	ost Group Name			Authorized Accounts							
	est			None. Authorize accounts							
<b>.</b> a	<sup>pi</sup>			None. Authorize accounts							
	Remove Bat	ch v					Total Items: 2	< Previous	1 Next >	Items per Pa	sge:20∨

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.

Bastionhost / Users / User Groups		
User Groups		
Create User Group Search by user group name Q		C
Name	Members	Actions
Operation Group	1	Authorize Hosts Authorize Host Groups
Test Group	0	Authorize Hosts   Authorize Host Groups
Delete		Total Items: 2 < Previous 1 Next > Items per Page: 20 ∨

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

← Op	peration G	Group				
Setting	s Members	Authorized Hosts	Authorized Host Groups			
Authori	ze Host Groups	Search by host group name	e Q			C
	Host Group Name		Authorized Accounts			
	test		None. Authorize accou	unts		
	арі		None. Authorize accou	unts		
	Remove Ba	tch 🗸		Total Items: 2	< Previous 1	Next > Items per Page: 20 \

**?** 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.

Bastionhost / Users / User Groups		
User Groups		
Create User Group Search by user group name Q		С
Name	Members	Actions
Operation Group	1	Authorize Hosts   Authorize Host Groups
Test Group	0	Authorize Hosts   Authorize Host Groups
		Total Items: 2 < Previous 1 Next > Items per Page: 20 V

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**.

< Op	eration	Group		
Setting	Member	rs Authorized Hosts Aut	thorized Host Groups	
Authoriz	e Host Groups	Search by host group name	٩.	С
đ	Host Group Nan	ne	Authorized Accounts	
	test	2 Batch Authorize Accounts	None. Authorize accounts	
	api	Batch Remove Authorized Accounts	None. Authorize accounts	
<b>~</b>	Remove	Batch 🗸	Total Items: 2 < Previous 1 Next > Items per Pag	ge: 20∨

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

Selected Host Groups: 2					
Accounts:	Enter the accounts you want to authorize				
Update					

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.

Bastionhos	t / Users / User Groups		
User	Groups		
Create I	Jser Group Search by user group name Q		С
	Name	Members	Actions
	Operation Group	1	Authorize Hosts Authorize Host Groups
	Test Group	0	Authorize Hosts   Authorize Host Groups
	Delete		Total Items: 2 < Previous 1 Next > Items per Page: 20 ∨

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

< Op	eratior	n Group						
Setting	is Membe	ers Authorized Hosts A	authorized Host Groups					
Authori	ze Host Groups	Search by host group name	Q					С
ă	Host Group Na	ame	Authorized Accounts					
~	test	Rately Authorize America	root					
<b>~</b>	арі	Batch Remove Authorized Account	root					
~	Remove	Batch 🗸		To	Total Items: 2	< Previous 1	Next >	Items per Page: 20 $\vee$

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

Batch Remove Authorized Accounts				
Selected Host Group	s: 2			
Accounts:	root			
Update				

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**.

Create A	uthorization Rule				
* Authoriz	zation Rule Name :				
					0
Validity Pe	eriod :				
Validity Pe	riod : Start date	~	End date	Ë	
Validity Pe Remarks :	riod : Start date	~	End date		

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.

sts				
	Batch Authori	ze Accounts		
С	Ent Batch Remove	e Authorized Accounts	/ 1 >	
Remov	ve Batch V	Associate Host Tota	al Items: 9 Selected Items: 1	1
	Host IP Address	Hostname	Operating System	Authorized Accounts
	192.168.2		Linux	
~	47.100.24	1.00	Linux	None. Authorize accounts
	192.168.2		Linux	100.00
	192.168.2		Linux	None. Authorize accounts
	101.132.2		Linux	None. Authorize accounts

- 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

> Document Version: 20220707

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.

Bastionhost / Policies / Control Policies / Create Control Policy			
Create Control Policy			
Basic Properties 2 Command Control 3 Command Approval 4	Protocol Control	5 Access Control	6 Result
Enter a single command and its arguments in each line. You can use the wildcard " to fuzzily match commands. Start a comment with a pound sign (#). Comments are not a part of the commands. Examples: 1: To match the config command, enter config. 2: To match commands that start with en, enter en" 3: To match ps commands with arguments, enter ps ". For example, enter ps " to match ps -aux. 4: To cutonize a regular expression to match any characters, enter REG." 5: To match any characters, enter "			
Command Control Type: (Blacklist) Listed Commands Are Not Allowed $\vee$			
Commands:			
	Previous: Basic Properties	Next: Command Approval	Create Control Policy

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.

Bastionhost / Policies / Control Policies / Create Control Policy			
Create Control Policy			
Basic Properties — Command Control — 3 Command Approval 4 Pro	otocol Control	Access Control	6 Result
Enter a single command and its arguments in each line. You can use the wildcard * to fuzzily match commands. Start a comment with a pound sign (#). Comments are not a part of the commands. Examples: 1: To match the config command, enter config. 2: To match commands with arguments, enter ps *. For example, enter ps * to match ps -aux. 4: To customize a regular expression to match any characters, enter REG.* 5: To match any characters, enter *			
Commands:			
A.			
	Previous: Command Control	Next: Protocol Control	Create Control Policy

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.

astionhost / Policies / Control Policies / Create Control Policy			
Create Control Policy			
create Control Policy			
Resis Presenting (1) Command Control (2) Command Annewal Annewal		a Control	G Result
basic Properties — O command control — O command Approval — O Protocol con	Acces	scontrol	6 Result
Enter a single IPv4 address or IPv4 address range in each line. For an IP address range, separate the start and end IP			
addresses with a hyphen (-), for example, 192.168.0.1 - 192.168.0.255. If you need to add a comment, start it with a pound sign (#) in a new line.			
Source IP Address Limit :			
(Blacklist) Listed IP Addresses Are Not Allowed			
IP Addresses :			
l			8
	Previous: Protocol Control		Create Control Policy
	Frevious, Frotocol Control		create control Policy

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.

Control Policies								
Create	Control Policy	Search by control policy name	Q					С
	Name	Users	User Groups	Hosts	Host Groups	Priority	Actions	
		0	0	0	0	1	Edit   Delete	
		0	0	0	0	1	Edit   Delete	
		0	0	0	0	1	Edit   Delete	
	Delete					Total Items: 3 < Previous	1 Next >	Items per Page: 20 $\vee$

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**.

Control Policy	/ Details						
← 123							
Control Policy Settings	Command Control	Command Approval	Protocol Control	Access Control	Host/User		
* Name							
			0				
Priority							
1			0				
Remarks							
		,					
Update Control Policy							

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.
| Control Policies      |                            |             |       |             |                        |                    |                |
|-----------------------|----------------------------|-------------|-------|-------------|------------------------|--------------------|----------------|
| Create Control Policy | Search by control policy r | name Q      |       |             |                        |                    | С              |
| Name                  | Users                      | User Groups | Hosts | Host Groups | Priority               | Actions            |                |
|                       | 0                          | 0           | 0     | 0           | 1                      | Edit   Delete      |                |
|                       | 0                          | 0           | 0     | 0           | 1                      | Edit   Delete      |                |
|                       | 0                          | 0           | 0     | 0           | 1                      | Edit   Delete      |                |
| Delete                |                            |             |       |             | Total Items: 3 < Previ | ous 1 Next > Items | per Page: 20 ∨ |

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.

Control Policies								
Create Control Policy Search by control policy name Q.								С
	Name	Users	User Groups	Hosts	Host Groups	Priority	Actions	
		1	0	2	0	1	Edit   Delete	
	-	0	0	0	0	1	Edit   Delete	
	10	0	0	0	0	1	Edit   Delete	

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.

← 123	
Control Policy Settings Command Control Command Approval Protocol Control Access Control Host/User	
Apply to All Hosts     Apply to Selected Hosts	
Hosts	Host Groups
C         Search by hostname or host         Q         1         /         1         >	C         Search by host group name         Q_         <
Remove Associate Host Total Items: 2 Selected Items: 0	Remove Associate Host Group Total Items: 0 Selected Items: 0
C Internet Street	

(?) 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.

Apply to All Users     Apply to Selected Users	
Users	User Groups
C Search by usemame or name Q < 1 / 1 >	C         Search by user group name         Q_i          1         / 0         >
Remove Associate User Total Rems: 1 Selected Rems: 0	Remove         Associate User Group         Total Items: 0         Selected Items: 0

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

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.

Bastionhost / Approval / Command Approval						
Command Approval						
Search by command Q Status: All V						С
Host	Protocol/Host Account	User/Source IP Address	Command	Requested/Approved At	Approved By	Status
C DESCRIPTION OF STREET, STREE	SSH roat	here a	Ш	May 28, 2020 3:17:35 PM May 28, 2020 3:17:44 PM		Rejected
<ul> <li>Prove the second se</li></ul>	SSH root	lines.	0	May 28, 2020 3:17:23 PM May 28, 2020 3:17:31 PM		Allowed

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.

Bastionhost / Approval / Command Ap	oproval						
Command Approv	val						
Search by command Q	Status: All						С
Host	Status: All 🗸	Protocol/Host Account	User/Source IP Address	Command	Requested/Approved At	Approved By	Status
	To Be Approved Canceled	SSH root	lines.	н	May 28, 2020 3:17:35 PM May 28, 2020 3:17:44 PM		Rejected
	Allowed Rejected	SSH root	have a	н	May 28, 2020 3:17:23 PM May 28, 2020 3:17:31 PM		Allowed

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

<sup>&</sup>gt; Document Version: 20220707

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

Bastionhost / Au	Bastionhost / Audit / Session Audit						
Session Audit							
All Sessions	Graphic Text Commands File Transfer						
Time :	All         Current Day         Current Month         Start date         ~         End date         =						
Protocol :	All	Host IP Address :	Enter a host IP address				
Hostname:	Enter a hostname	User:	Enter a username				
Logon Name:	Enter a logon name	Source IP Address:	Enter a source IP address				
Session ID:	Enter a session ID						
	Search Reset						

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: <b>All</b> , <b>Current Day</b> , <b>Current Week</b> , and <b>Current Month</b> . 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	<ul> <li>Select a session deletion state. Valid values:</li> <li>All</li> <li>Undeleted</li> <li>Deleted</li> </ul>

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.

Туре	Host	Protocol/Logon Name	User/Source IP Address	Start Time/End Time	Session Duration/Size	Actions
SHELL	1000	SSH root	Trans.	May 28, 2020 3:17:21 PM May 28, 2020 6:38:59 PM	3 Hours 21 Minutes 38 Seconds 1.05KB	Play Details
SHELL	A CONTRACTOR OF A	SSH root	and the second	May 28, 2020 3:16:23 PM May 28, 2020 6:39:01 PM	3 Hours 22 Minutes 38 Seconds 1.11KB	Play   Details
RDP	1000	RDP administrator	5	May 28, 2020 2:54:22 PM May 28, 2020 2:55:25 PM	1 Minutes 3 Seconds 2.34MB	Play   Details

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

Session Details						
Session ID	14ef39475ecf65810000000000000	015				
Session Duration	3 Hours 21 Minutes 38 Seconds	Session Size	1.05KB			
Start Time	May 28, 2020 3:17:21 PM	End Time	May 28, 2020 6:38:59 PM			
User	zly	Source IP Address	1000			
Source Port	33500					
Hostname		Host IP Address				
Logon Name	root	Protocol	SSH			
Host Port	22					

## 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.

Туре	Host	Protocol/Logon Name	User/Source IP Address	Start Time/End Time	Session Duration/Size	Actions
SHELL	10.00	SSH root	The second second	May 28, 2020 3:17:21 PM May 28, 2020 6:38:59 PM	3 Hours 21 Minutes 38 Seconds 1.05KB	Play   Details
SHELL	A CONTRACTOR OF A	SSH root	Trans.	May 28, 2020 3:16:23 PM May 28, 2020 6:39:01 PM	3 Hours 22 Minutes 38 Seconds 1.11KB	Play   Details
RDP	1000	RDP administrator	E.c.	May 28, 2020 2:54:22 PM May 28, 2020 2:55:25 PM	1 Minutes 3 Seconds 2.34MB	Play   Details

## 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.

ActionTrail	Operations Log			Central (?) 180 Days
👩 OSS	Access Log			Regional ⑦ 7 Days 180 Days
	Metering Log			Central (?) 180 Days
😵 RDS	SQL Audit Log 🕜	Disabled	Collection Policy	Central (?) 180 Days
	Slow Query Log Public Preview	Disabled	Collection Policy	Central (?) 180 Days
	Performance Log Public Preview	Disabled	Collection Policy	Central (?) 180 Days
🍞 PolarDB	Audit Log (?)	Disabled	Collection Policy	Central (?) 180 Days
	Slow Query Log Public Preview	Disabled	Collection Policy	Central (?) 180 Days
	Performance Log Public Preview	Disabled	Collection Policy	Central (?) 180 Days
🔗 PolarDB-X	SQL Audit Log	Default	Collection Policy	Regional 7 Days 180 Days
👃 SLB	Lay-7 Access Log	Default	Collection Policy	Regional 7 Days 180 Days
Bastion Host Public Preview	Operations Log			Central ⑦ 180 Days
🕼 Web Application Firewall	Access Log 🕐			Central ⑦ 180 Days
( Cloud Firewall Public Previewall	Internet Access Log 📀			Central ⑦ 180 Days
lig Anti-DDos Public Preview	Anti-DDoS Pro Access Log (?)			Central ⑦ 180 Days
Security Center(SAS)	Configure Log Subcategories			Central ⑦ 180 Days

- 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.

Session Audit							
All Sessions	Graphic Text	Commands	File Transfer	Log Backup			
Name			File Size		Backup Start Time	Backup End Time	Actions
2021-09.csv			0.11MB		September 1, 2021	September 30, 2021	Download
2021-08.csv			14.05KB		August 1, 2021	August 28, 2021	Download
2021-07.csv			6.41KB		July 1, 2021	August 1, 2021	Download
2021-06.csv			3.88KB		June 1, 2021	July 1, 2021	Download
2021-05.csv			34.08KB		May 4, 2021	June 1, 2021	Download

## 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.

Bastionhost / Audit / R	eal-Time Monitoring				
Real-Time N	Monitoring				
ited inite i	lionitoring				
Protocol :	All		Host IP Address:	Enter a host IP address	
Hostname :	Enter a hostname		User:	Enter a username	
Logon Name :	Enter a logon name		Source IP Address:	Enter a source IP address	
Session ID :	Enter a session ID				
	Search Reset				
Filters :	Clear Save				Default Condition

- 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.

Bastionhost / Au	udit / F	Session Detail	s			×	
Real-Tir	Real-Time						
		Session ID	31	000034			
Protocol :	All	Session Duration	0 Seconds	Session Size	OB	ess	
Hostname :	Enter a	Start Time	June 4, 2020 3:33:24 PM	End Time	-		
L							
Logon Name :	Enter	User	test	Source IP Address	-	dress	
	Lincer	Source Port	1000				
	Searc						
Filters :	Clear	Hostname	10000	Host IP Address	10.000		Default Condition
Туре		Logon Name	root	Protocol	SSH	ne/Duration	Actions
SHEL	L	Host Port	22			2020 3:33:24 PM nds	Play   Details
Int	terrupt §					Previous 1	Next > Items per Page: 20 V

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.

Bastionhost / A	udit 7 Real-Time Monitoring				
Real-Ti	me Monitoring				
Protocol :	All	$\vee$	Host IP Address	Enter a host IP address	
Hostname :	Enter a hostname		User:	Enter a username	
Logon Name :	Enter a logon name		Source IP Addre	Enter a source IP address	
Session ID :	Enter a session ID				
	Search Reset				
Filters :	Clear Save				Default Condition $\qquad \lor$
🗸 Туре	e Host	Protocol/Logon Name	User/Source IP Addre	ess Start Time/Duration	Actions
✓ RDP	THE REPORT OF THE	RDP administrator		May 18, 2020 2:15:31 PM 20 Seconds	Play Details

## 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.

	Туре	Host	Protocol/Logon Name	User/Source IP Address	Start Time/Duration	Actions
<b>~</b>	RDP		RDP administrator	Sec	May 18, 2020 2:15:31 PM 20 Seconds	Play   Details
~	Interru	pt Sessions		Total	Items: 1 < Previous 1 Next 2	> Items per Page: 20 V

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: <b>All</b> , <b>Current Day</b> , <b>Current Week</b> , and <b>Current Month</b> . You can also specify a custom time range.
------	---

Result	<ul> <li>Select the result of the operation that you want to view from the Result drop-down list. Valid values:</li> <li>All</li> <li>Successful</li> <li>Failed</li> </ul>
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.

08	O&M Reports				
Date	Current Day Previous Day Current Week Curr	ent Month 2021-08-12 00:00:00 ~ 2021-08-12 09:05:50	0	Expor	rt Report 🗸
0	Verview Session Size O&M Operations	O&M Duration			
	Overview		O&M Operations		
	Hosts for O&M	0	Total O&M Operations	0	
	Source IP Addresses for O&M	0	SSH	0	
	O&M Users	0	RDP	0	
			SFTP	0	
			Daily O&M Operations on Average	0.0	
	O&M Duration		Session Size		
	Total O&M Duration	0 Seconds	Total Session Size	OB	
	SSH	0 Seconds	SSH	0B	
	RDP	0 Seconds	RDP	OB	
	SFTP	0 Seconds	SFTP	OB	
	Daily O&M Duration on Average	0 Seconds	Daily Session Size on Average	OB	
	Maximum O&M Duration	0 Seconds	Maximum Session Size	OB	
	Minimum O&M Duration	0 Seconds	Minimum Session Size	OB	(

#### 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.

#### **Bastion Host**

Verview Session Size O&M Operations O&M Duration						
Trend Chart						
Hourly Daily Weekly Monthly	Hourly Daily Weekly Moenthly					
Count						
1						
	August 12, 2021 SSH 0 RDP 0					
SFIP     O     Total     O						
0 August 12, 2021	0 August 12, 2021					
💊 SSH 💊 RDP 💊 SFTP 🔩 Total						

#### **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.

Overview Session Size O&M Operations O&M Duration	
Trend Chart	
Hourly Dualy Weekly Monthly	
Duration	
s 40 Seconds	
zes 0 Seconds	
s 20 Seconds	
s 40 Seconds	Å J
March 1, 2021 March 24, 2021 April 16, 2021 May 9, 2021 June 1, 2021 June 24, 2021 Jun	gust 12, 2021 Time
💊 SSH 💊 RDP 💊 SFTP ∿ Total	

#### **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.

O&M Reports							
Date:	Current Day	Previous Day	Current Week	Current Month	2021-03-01 00:00:00 ~ 2021-08-12 09:11:23	Export Report 🗸	
Oven	iew Se	ssion Size	O&M Operations	O&M Duration			
Tren	l Chart						

# 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

licon in the Log On column. The host O&M page appears.

Host O&M						
Search by hostname or host IP Q	Operating System: All $\sim$	Host Source: All $\qquad \lor$				
Hostname	Host IP Address	Remarks	Operating System	Host Source	Host Account	Log On
wb	172.16.43		Linux	ECS	[SSH] root V	۲
banne	192.16		Linux	ECS	[SSH] root $\lor$	۲
bann	192.168.		Linux	ECS	[SSH] root $\lor$	۲
win	116.62.21		Windows	ECS	No Authorized Host Accounts	۲
linux	121.43.22		Linux	ECS	[SSH] root V	۲
1.1		APItest	Windows	Local	No Authorized Host Accounts	

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 settings1.11.1. Configure the parameters on the UserSettings 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.

- 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 <b>0</b> , 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 <b>0</b> , an account is locked until the administrator unlocks the account.

Parameter Account Lockout Policy		
		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 <b>Account Lockout</b> <b>Threshold</b> . Unit: minutes.
	Reset Account Lockout Counter After	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 <b>0</b> , 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 <b>0</b> , 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.

vo-Factor Authentication		
Enable Two-factor Authentication		
* Authenticat ✔ Text Message		
🗸 Email		
V DingTalk		
* AppKey: dinge		
* AppSecret: QX984		
* Agentid : 18		
Send Test Message		
Language: ④ 简体中文 🔵 English		
If the two-factor code is correct, you do not need to enter the code for	Hours	0
Save		

## 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.

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

curity Configuration	Two-Factor Authentication	AD Authentication	LDAP Authentication		
Server Address :					
tandby Server Address :					0
Port:	0				
SL:					
Base DN :					
Domain :					
Account:					
Password :				e ø	
ilter:					0
Jame:					0
mail:					0
Aobile Number:					0

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.

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

curity Configuration	Two-Factor Authentication	AD Authentication	LDAP Authentication		
Server Address :					
tandby Server Address :				0	
Port:	636				
SL:					
* Base DN :		insulation in the second s			
* Account:		CONTRACTOR OF CONTRACTOR			
Password :			Time 5	ð	
ilter:	(&(ob	jectClass=*))		0	
ogon Name Attribute :				0	
lame :				0	
mail :				0	
Ashila Number					

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.

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

Bastionhost / System Settings	as				
Security Configuration	Two-Factor Authenticat	on AD Authentication	LDAP Authentication	O&M Configuration	Network Diagnosis
Connectivity Test					
* Target IP Address :					
* Port:	80				
	Test	Connection			

#### 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.

Security Configuration Two-Facto	r Authentication	AD Authentication	LDAP Authentication	O&M Configuratio
O&M Configuration				
Special Host Account :	<ul> <li>Allow Acc</li> </ul>	ess to Hosts by Using Bast	ionhost Account and Password	0
	Allow Acc	ess to Hosts by Using Una	uthorized Host Accounts 💿	
Special Host Configuration :	Allow Ho	st Fingerprinting ③		
Idle Timeout Interval :	0	Minutes (2)		
Duration Limit :	30	Hours ()		
Duration to Lock Hone Hone Consider Block	a (Unit 1	Minuter		

The following table describes the parameters.

Parameter	Description
-----------	-------------

Parameter	Description
	<ul> <li>Valid values:</li> <li>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.</li> </ul>
	<b>Note</b> 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.
Special Host Account	<ul> <li>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.</li> </ul>
	<b>Note</b> 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.
	<ul> <li>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&amp;M.</li> </ul>
	Specifies whether to enable the host fingerprint feature. The host fingerprint feature is enabled by default.
Special Host Configuration	<b>Note</b> 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	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.
Interval	<b>Note</b> In an <b>idle O&amp;M session</b> , 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.

Storage Status		
Storage Status:	(	1%
	82.40MB / 2TB	

## Configure automatic deletion of session data

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

Automatic Deletion				
Automatic Deletion:	Maximum Session Data Storage Duration	180	Days	0

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.

8	2.40MB	/ 2TB					
	August	24, 20	21 9:43	3:34 AN	1		
	<< <		A	ug 202	1		> >>
	Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6	7
	8	9	10	11	12	13	14
	15	16	17	18	19	20	21
	22	23	24	25	26	27	28
ŀ.	29	30	31	1	2	3	4
	5	6	7	8	9	10	11
	Now				selec	t time:	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.

Notification			
Command Alert Notification 🧿			
Storage Capacity Notification ③			
Notifications of Automatic Tasks ③			
O&M Report Notification ③			
Shared Key Expiration Notification	180	Days	0
Save			

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	If storage space will be used up soon, for example, 85% of the storage space is used, Bastionhost notifies you by internal message.
Notification	(?) <b>Note</b> If the remaining storage space remains unchanged or keeps decreasing, Bastionhost no longer notifies you.
	If an automatic password change task is complete, Bastionhost notifies you by internal message.
Notifications of Automatic Tasks	<b>Note</b> 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.
	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.
Shared Key Expiration Notification	<b>Note</b> 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 silon in the upper-right corner of the Bastionhost console to go to the **Message** 

Center. In the Message Center, you can view your notifications.

ckets	ICP	Enterprise	Support	App	>_	۵.	Ä
Sit	e Mes	sages		Messa	ge Seti	tings	
12			-				
2							
	-						
-							

## 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 to a bastion host that can manage 50 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.

# 2.0&M manual 2.1. 0&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.

Properties of New Session				?	$\times$
Category:					
- Connection	Connection				
- Authentication	General				
Login Scripts	Name:	New Session		_ <b>_</b>	
SSH	Protocol:	SSH	~		
- <b>Tunneling</b>	Host:	wiveh-	.com		
	Port Number:	60022			
SERIAL	Description:		^		
Keep Alive			$\sim$		
< Keyboard	Reconnect				>
Advanced	Reconnect au	tomatically if connection is	terminated unexpec	tedly	
- Appearance Window	Interval:	0 sec	Limit: 0	^ min	
Highlight		<b>v</b>		T	
Trace	TCP Options				
Bell Logging	Use Nagle's a	lgorithm			
File Transfer					
		Connect	ОК	Cancel	

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

				-	
Properties of New Session				?	X
Category:					
- Connection	Connection > A	uthentication			
- Authentication	Select an authent	ication method and other re	elated parameters.		
-Login Scripts	Use this section to	o save time when logging in	. However, for max	imum securit	ty, we
SSH	recommend you l	eave this section blank if sec	curity is a concern.		
- Security					
SFTP	Mashada	Pacquard	~	<u> </u>	
TELNET	Method:	Fassword	Ť	Setup	
- RLOGIN - SERIAL	User Name:	-			
Proxy	Password:	•••••			
Keep Alive	User Key:	<none></none>	~	Browse.	
< Keyboard	Pacenhrace				>
-VT Modes	rasspillase.				
- Advanced					
Window					
-Highlight					
Trace					
-Bell					
Logging – File Transfer					
-X/YMODEM					
ZMODEM					
		Connect	ОК	Cance	el

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**.

Two-Step Vertication failure, please try again							
23	Place Input Short Message Code:						
	******						
	Remember Password						
	OK Cancel						

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.

 Quit: Use ":q <enter>". Move: Use the cursor keys, or "j" to go down, "k" to go up, "u" to PageUp, "p" to PageDown. Search: Use "/{patten}<enter>" and then "n"/"N" to next/privous searching result. Jump: Use ":{number}<enter>" to jump to line {number}. Command: Use ":[ssh telnet rlogin] [-l user] {user}@{host}:{port} [-p port]<enter>" for login. Use ":[ping traceroute connect] {host} [port]<enter>" for check host status.</enter></enter></enter></enter></enter>
 Refresh: Use "r" to refresh lists.
 Language: Use "e" to change language encoding between UTE-8 and GB2312.
[usmshell] 001:linux 101 22 ssh root

## 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.



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

Semote Desktop Connection — 🗌 🗙						
	Remote Desktop Connection					
<u>C</u> omputer:		· · · · ·				
User name: None specified						
You will be asked for credentials when you connect.						
Show O	ptions	Co <u>n</u> nect	<u>H</u> elp	)		

3. In the **Remote Desktop Connection** dialog box that appears, click **Yes**.
| 褁 Rei            | mote Desktop Connection   | ×     |
|------------------|---|-------|
| $\bigcirc$       | The identity of the remote computer cannot be verified. Do you war connect anyway?                              | nt to |
| The re<br>securi | emote computer could not be authenticated due to problems with its ty certificate. It may be unsafe to proceed. |       |
| Name             | e mismatch  |       |
| 1                | Requested remote computer:<br>dkeinwiveh-public.bastionhost.aliyuncs.com  |       |
|                  | Name in the certificate from the remote computer:<br>BAOLEIJI   |       |
| Certif           | ïcate errors  |       |
| The<br>com       | following errors were encountered while validating the remote<br>nputer's certificate:                          |       |
| <u>^</u>         | The server name on the certificate is incorrect.  |       |
| Â                | The certificate is not from a trusted certifying authority.   |       |
| Do yo            | u want to connect despite these certificate errors?   |       |
| 🗌 Do             | n't ask me again for connections to this computer   |       |
| View             | w certificate Yes No  |       |

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

🗐 login		
username <sup>.</sup>		
username.		
password:	*****	
	Login	Cancel

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**.

<u> </u>	ogin
	🗐 Two Factor
user	Place Input Short Message Cod e:
pas	
	Ok Cancel
	L L L L L L L L L L L L L L L L L L L

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

🗇 Ma	nin					
Chan	ge Password	New connectio	on			Logout
No.	Hostname		IP		Username	Port
1					administrator	3389
2			1000		[empty]	3389
	First	Previous	1/1	Next	Last	

# 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.

operties of New Se	ession	? ×
General Options		
Sito		
Site		
Name:	New Session	
Host:	ubliccom	
Protocol:	SFTP v	Setup
Port Number:	60022	
Proxy Server:	<none> ~</none>	Browse
Description:		^
		$\checkmark$
Login		
Anonymous log	jin	
Use authentica	tion agent	
Method:	Password v	Setup
User Name:	100 C	
Password:	•••••	
User Key:	<none></none>	Browse
Passphrase:		
	Connect C	OK Cancel

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**.

Two-Step	Vertication failure, plea	ase try again	×
23	Place Input Short Message	e Code:	^
			~
	*****		
	Remember Password		
		ОК	Cancel

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

💐 Desktop - test@rtka	yfrhnm-public.bastionhost.aliyuncs.com	m - WinSCP		-	0 X
the second has	CARLES DEPARTURE AND A				
🕀 🈂 🐂 🔳 🤞	P 📭 🐵 🔊 🖬 🔹 🖬 🖬 🖬	• 🍠 •			
🖵 test@rtkayfrhnm-p	ublic.bastionhost.aliyuncs.com 🛛 🔛 🖷				
💶 - 🗂 - 🕎 - 👔			<b> </b> / • ≝ • ▼ • 🖨 🗁 🖓 🚵 ■ ■ 🔚 ← • → •		
	× 🛛 🕞 🚞 🚔 🔲 🗉 🗑	✓	i 🖉 💷 - 🛛 🖉 🔜 - 🗙 🖓 🕞 📖  🖆 🔜 🖬 🗉 🖼		
C:\Users\jialin\Desktop\			/		
· · ·	1.1. BOX		^ ^	 1000	
📕 🗋	202	20/6/4 15:22:59	L		
	20	20/6/4 11:56:52	Inow_gb18030,next_UTF-8	2020/6/4	15:38:59
é.	27 KB Microsoft Excel I 20	20/6/3 14:45:05	ssh_root@121.40.190.52:22	2020/6/4	15:38:59
<b>6</b>	700 KB Microsoft Word 20	20/6/4 11:53:29			
۵	14 KB Microsoft Excel T 20	20/6/3 11:16:17			
ž	105 KB XMind Workbook 20	20/6/1 23:11:32			

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.

stionhost / Overview					
Statistics Overview				O&M Portals	
A Users	象 User Groups	🖵 Hosts	🖁 Host Groups	Internet	
1	2	2	2	Private Network	0
D&M Statistics					
4		~		Real-Time Sessions	Vie
2				Real-Time Connections	
3				Remaining Connections	5
2				A stive Users	
1				Active Users	
0					
May 24, 2020 N	1ay 25, 2020 May 26, 2020 N	1ay 27, 2020 May 28, 2020 1	May 29, 2020 May 30, 2020	Command Sessions	
	∿ Total ∿ File Transfer Sessio	ons 🔹 Graph Sessions 🔹 Co	mmand Sessions	Graph Sessions	
				THE TRACE	

### Procedure

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

•	🏦 admin — ssh zha	shi@yll	.com -p60022	2 — 101×24
admindeMac-m	ini:~ admin\$ ssh zha	shi@yll	the second second second second	.com -p60022
zha	shi@yll		s.com's password: 🝸	

- 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.

• • •	🟦 admin — ssh zhang	shi@ylbn	aliyuncs.com -p60022 — 101×24
[admindeMac-mini:~	admin\$ ssh zhang	shi@yll	:.aliyuncs.com -p60022
[zhang shi@y]	16	.aliyuncs.com's	password:
Two-Step Vertifica	ation required		
Please enter the M	MFA verification cod	le:	

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.

۲			admin — USMShell — ssh zhang shi@ylb .aliyuncs.com -p60022 — 101×24	
	Quit: Move: Search: Jump: Command: Refresh: Language:	Use Use Use Use Use Use Use Use	<pre>":q<enter>". the cursor keys, or "j" to go down, "k" to go up, "u" to PageUp, "p" to PageDown. "/{patten}<enter>" and then "n"/"N" to next/privous searching result. ":{number}<enter>" to jump to line {number}. ":[ssh telnet rlogin] [-1 user] {user}@{host}:{port} [-p port]<enter>" for login. ":[ping traceroute connect] {host} [port]<enter>" for check host status. "r" to refresh lists. "e" to change language encoding between UTF-8 and GB2312.</enter></enter></enter></enter></enter></pre>	
	[usmshell 001: ]	] _1:	inux 101.5 1223:22 ssh root	

### 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.

Microsoft*
,: ylbnaliyuncs.com:6

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

****
Login Cancel

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**.

🖹 la	ogin	
	Two Factor	
	Place Input Short Message Cod	
user	e:	
pase		
	Ok Cancel	

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

🖹 Ma	ain					
Chan	ige Password	New connecti	on			Logout
1						
No.	Hostname		IP		Username	Port
1					administrator	3389
2					[empty]	3389
	First	Previous	1/1	Next	Last	

# 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.

onhost / Overview					
atistics Overview				O&M Portals	
Users	象 User Groups	🖵 Hosts	器 Host Groups	Internet	
	2	2	2	Private Network	
&M Statistics					
4				Real-Time Sessions	۷
3				Real-Time Connections	
2				Remaining Connections	
				Active Users	
0				Active Hosts	
May 24, 2020	May 25, 2020 May 26, 2020 N	lay 27, 2020 May 28, 2020 N	1ay 29, 2020 May 30, 2020	Command Sessions	
		ne 💁 Graph Sociene 💁 Con	amand Serrions		
	∿ Total ∿ File Transfer Sessio	ris • Graph Sessions • Con		Graph Sessions	

### Procedure

1. Start the SecureFX tool.

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

0.00		💯 SecureFX		
* 1				
Connect Syn Ze Download	Refresh Stop Folder Tree Sync Browsing			Connect Bar
Scal (admindeMac-mini.k	ocal)			
1				✓ Filter <%F> ✓
▼ 🖻 /	Name	Size Type	Date Modified	
DocumentRevis	DocumentRevisions-V100	Directory	10/14/19 14:40	
.fseventsd	ifseventsd	Directory	10/14/19 15:26	
PKInstallSandb	.PKInstallSandboxManager	Directory	09/27/18 12:43	
PKInstallSandb	PKInstallSandboxManager-Sy	Directory	10/14/19 14:39	
.Spotlight-V100	Spotlight-V100	2 Directory	09/27/18 12:43	
iov. 📄	ivol	Directory	08/18/18 07:13	
Applications	Applications		10/14/19 15:26	
in bin	bin	2 7 + % □ □ × ☆ ň ⊡ »	10/14/19 14:38	
cores	cores		10/14/19 17:35	
▶ 🔤 dev	e dev	Filter by session name <%1>	10/14/19 14:40	
▶ etc	etc	Sessions	10/09/19 10:41	
me home	home		10/14/19 15:04	
Library	Library		09/30/19 12:34	
🕮 net	met net		10/14/19 15:04	
Network	Network		08/18/18 07:13	
private	private	Show dialog on startup	09/27/18 08:04	
i sbin	sbin	Close	10/14/19 14:38	
System	System	close	09/2//18 08:01	
▶ 💼 tmp	tmp	Directory	10/14/19 15:44	
Users	Users	Directory	11/30/18 14:25	
▶ 🛄 usr	usr	Directory	09/27/18 07:53	
▶ 🔜 var	var	Directory	11/30/18 14:26	
vm	vm	Directory	10/14/19 14:38	
28 entries (plus 2 hidden entr	ies)			
8		Transfer Queue		
Filename D	Destination Size of File 3ytes Transferred	Progress Elapsed Time Time Left Speed Status	Start Time	Finish Time

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.

	💯 Session Options - New
Category:	SSH2
▼ Connection ▼ SSH2	Hostname: ylbnaliyuncs.com Port: 60022
Advanced ▼ File Transfer FTP/SFTP Advanced	Firewall: None
	Username: zhar
	✓       PublicKey       ▲       Properties         ✓       Keyboard Interactive       ▼       ▼         ✓       Password       ▼       ▼         ✓       GSSAPI       ▼       ▼
	Key exchange         Image: Construction of the state of the stat
	Minimum group exchange prime size: 2048
	Cancel OK

4. Select the created bastion host and click Connect.

	💯 Con	nect					
0 4 <b>+</b> X	o 🗅		× 🌣	- Ä	÷	>>	
Filter by session name	e <%l>					8	
Sessions     New							
✓ Show dialog on startup							
		С	lose	C	onnec	t J	

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

ylbr requires a p	aliyuncs.com. assword. Please enter a password now.	ОК
Username:	zhanç shi	Cancel
Fassword:	•••••	
Save pas	ssword	Skip

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.

💿 💿 💿 🌠 Two-Step Vertification required Authent	tication
Two-Step Vertification required prompt for zhang shi@ylbr .aliyuncs.com.	OK
Please enter the MFA verification code:	
03 Save password	Skip

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.

	🗐 Se	cureFX				
Connect Synchronize Download Refresh Stop Folder Tree Sync Browsing		0 7 111			Connect Bar	
	v Filter <%F> v	1			▼ Filter <%F>	•
V     /       g. DocumentRevisions     //       g. PKInstallSandb     //       g. Spotlight-V100     //       y. Vol     //       bin     cores       idev     idev       im home     ibin       im ktwork     ibin       private     private       sbin     System       bin     System	Size	v in /	Name Inow ssh_ro	Size Type Directory Directory	Date Modified 10/14/19 17:52 10/14/19 17:52	
Image: Series     Image: Series       Image: Series     I		i SEND : RealPath, base=. i Resolved RealPath: / < drwxr-xr-x 4096 Mon 14-Oct < drwxr-xr-x 4096 Mon 14-Oct	2019 17:52:17 !now_gb18030, 2019 17:52:17 ssh_root@±¤Åi	next_UTF-8 (S) fwû-linux_101 2	23:22 (5)	0
28 entries (nlus 2 hidden entries)		2 entries				
8	Trans	fer Queue				
Filename Destination Size of File 3ytes Transfer	ed Progress Elapsed Time Time Let	t Speed Status	Start Time	Finish Time		