ALIBABA CLOUD

Alibaba Cloud

Bastion Host

FAQ

Document Version: 20220606

Alibaba Cloud

Legal disclaimer

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

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

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

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

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

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

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

Document conventions

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

Table of Contents

1.FAQ related to feature usage

This topic provides answers to some frequently asked questions about Bastionhost.

Bastionhost provides more features and constantly improves user experience by rolling out scheduled version updates. Features vary among different versions of bastion hosts. For more information, see Versions and documents. FAQ is divided into the following sections based on different versions of bastion hosts:

- FAQ about all versions of Bastionhost
  - Can I use a key pair for authentication when I log on to a bastion host in SSH mode?
  - Can I directly connect to the IP address of an ECS instance after I purchase a bastion host?
  - What are the configurations to allow O&M personnel to access an ECS instance only from a bastion host?
  - What do I do if an access failure message appears after I log on to a bastion host and attempt to access an ECS instance from the bastion host?
  - What do I do if the error message shown in the following figure appears when I use WinSCP to log on to an SFTP server?
  - I am prompted to enter a password when I use a private key to access an ECS instance. What do I do?
  - What do I do if I cannot access an ECS instance from my bastion host?
  - If I am an O&M engineer, how do I change the password to log on to a bastion host?
  - What ports are enabled for a bastion host? Can I change these ports?
- FAQ about Bastionhost V3.2
  - How do I store the O&M logs of Bastionhost in Log Service?
  - How do I allow the egress IP addresses of a bastion host in a security group of an ECS instance?
  - How do I access an ECS instance from my bastion host by using an internal IP address?
  - How do I configure my bastion host if I want to access an ECS instance by using a port other than the SSH- or RDP-compliant standard port?
  - How long can audit videos in a bastion host be stored?
  - If I use an RDP-based client, how do I switch to another host to perform O&M operations?
  - How do I configure a server as an HTTP or SOCKS5 proxy server?

Can I use a key pair for authentication when I log on to a bastion host in SSH mode?

Yes, you can use a key pair or a password for authentication when you log on to a bastion host in SSH mode over port 60022.

For more information about how to use a key pair to log on to a bastion host, see Host the public key of a user.

For more information about how to log on to a bastion host in SSH mode, see one of the following links based on your operating system:

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

Can I directly connect to the IP address of an ECS instance after I purchase a bastion host?

By default, no control policies on IP addresses of Elastic Compute Service (ECS) instances are configured on bastion hosts. If an access control policy on the ECS instance is not configured, you can connect to the IP address of the ECS instance.

> **Note** To ensure the compliance and integrity of server O&M, we recommend that you configure access control policies to allow only bastion host-based O&M operations on the ECS instance. For more information about how to configure access control policies, see Create a control policy.

What are the configurations to allow O&M personnel to access an ECS instance only from a bastion host?

You can configure a security group for the ECS instance to allow access only from the IP address of the bastion host. You can also save logon credentials only in the bastion host instead of disclosing the credentials to the O&M personnel. This way, the O&M personnel can access the ECS instance only from the bastion host. For more information about how to configure a security group, see Add a security group rule.

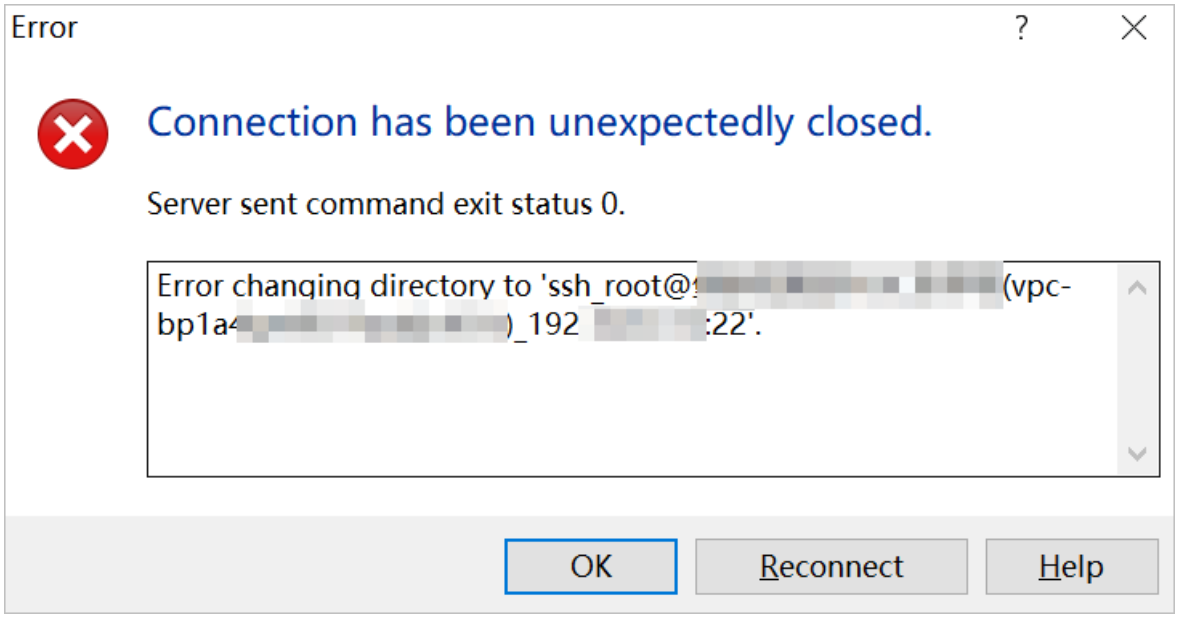
What do I do if an access failure message appears after I log on to a bastion host and attempt to access an ECS instance from the bastion host?

Check the firewall settings and the security group of the ECS instance. Make sure that no access control rules are configured to prohibit access to the ECS instance over the O&M port from a bastion host.

What do I do if the error message shown in the following figure appears when I use WinSCP to log on to an SFTP server?

Problem description

When I use WinSCP to log on to an SFTP server, the error message appears, as shown in the following figure.



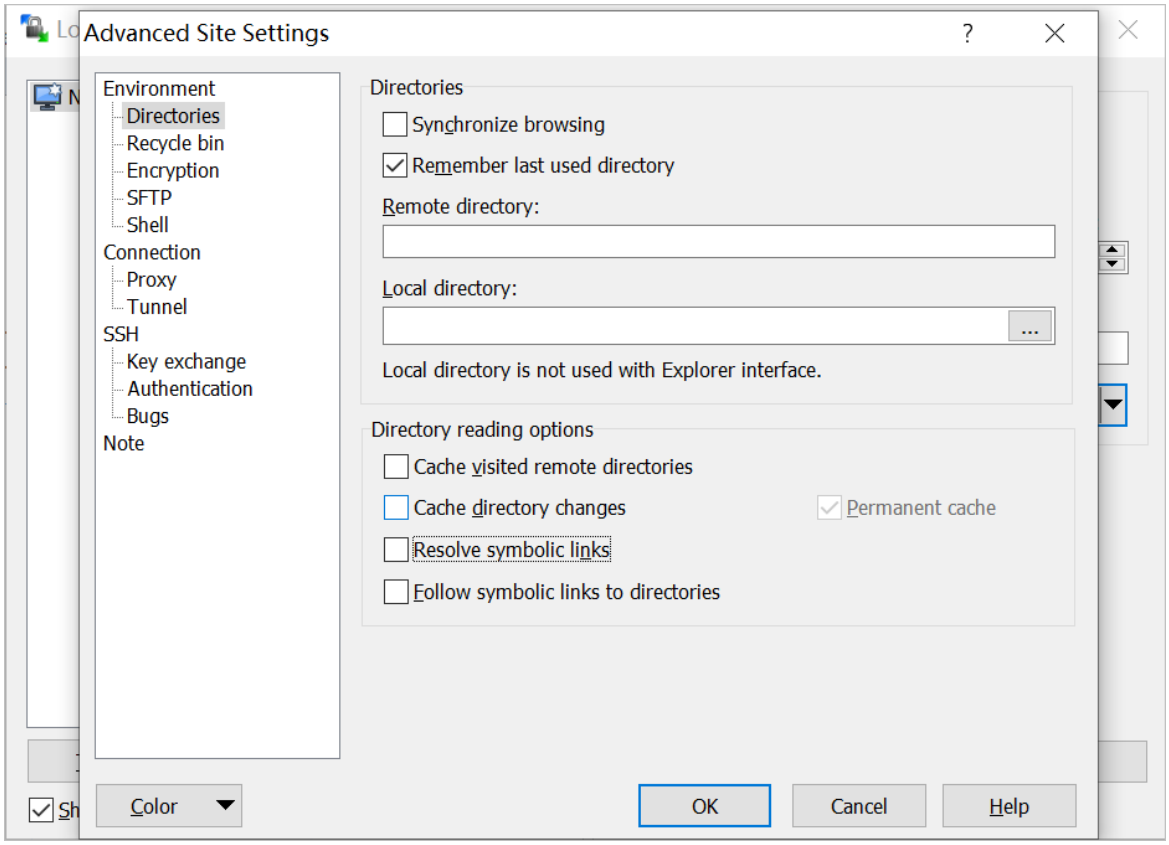
Cause

The error message appears because of the caches on WinSCP.

Solution

If the error message appears because of the caches on WinSCP, you must perform the following steps on WinSCP:

1. Open WinSCP.
2. In the left-side navigation pane, choose **Environment > Directories**.
3. In the **Directory reading options** section, clear all options.



4. Click **Save**.
5. In the server list, click the SFTP server to log on to the server again.

I am prompted to enter a password when I use a private key to access an ECS instance. What do I do?

You can perform the following operations to troubleshoot this issue:

1. Check the type of your private key. You can access an ECS instance from your bastion host only by using a Rivest-Shamir-Adleman (RSA) private key that is generated by the ssh-keygen tool. The private key does not contain a password.

2. You can use a private key to access an ECS instance and check whether valid credentials are added to the required authorized groups. For more information about how to configure a private key for a bastion host that runs V3.2, see Set a private key for an account.

What do I do if I cannot access an ECS instance from my bastion host?

You can perform the following operations to troubleshoot this issue:

- Check the connection that is established between your bastion host and the ECS instance. Make sure that your bastion host can be connected to the ECS instance. For more information about how to check the connection that is established between a bastion host and an ECS instance, see Diagnose network issues.
- Check whether the security group rules of the ECS instance are properly configured. Make sure that you can access O&M ports of the ECS instance from your bastion host.
- Check whether access control limits, such as iptables, exist on the firewall of the ECS instance or

other intermediate devices.

- Check the port information that is used to access the ECS instance in Bastionhost. Make sure that the added credentials, such as the username, the key pair, or the password of the ECS instance, are valid.

If I am an O&M engineer, how do I change the password to log on to a bastion host?

You can use one of the following methods to change the password to log on to a bastion host:

- Contact the administrator of the bastion host.
- Log on to the bastion host and change the password.

What ports are enabled for a bastion host? Can I change these ports?

The following ports are enabled for a bastion host by default:

- HTTPS port 443 in a web console
- SSH-compliant O&M port 60022
- RDP-compliant O&M port 63389

> **Note** You cannot change these ports in Bastionhost V2 and V3.1. You can change these ports in Bastionhost V3.2. Ports 1 to 1024 are reserved for Bastionhost. Do not change the ports that are enabled for a bastion host by default to reserved ports.

How do I store the O&M logs of Bastionhost in Log Service?

You can store the O&M logs of Bastionhost in a specific Logstore in Log Service. The O&M logs of Bastionhost record O&M operations that O&M engineers perform by using bastion hosts. After the O&M logs of Bastionhost are configured to be stored in Log Service, Bastionhost delivers and stores the O&M logs in the specific Logstore in Log Service. You can perform the following steps to store the O&M logs of Bastionhost in Log Service:

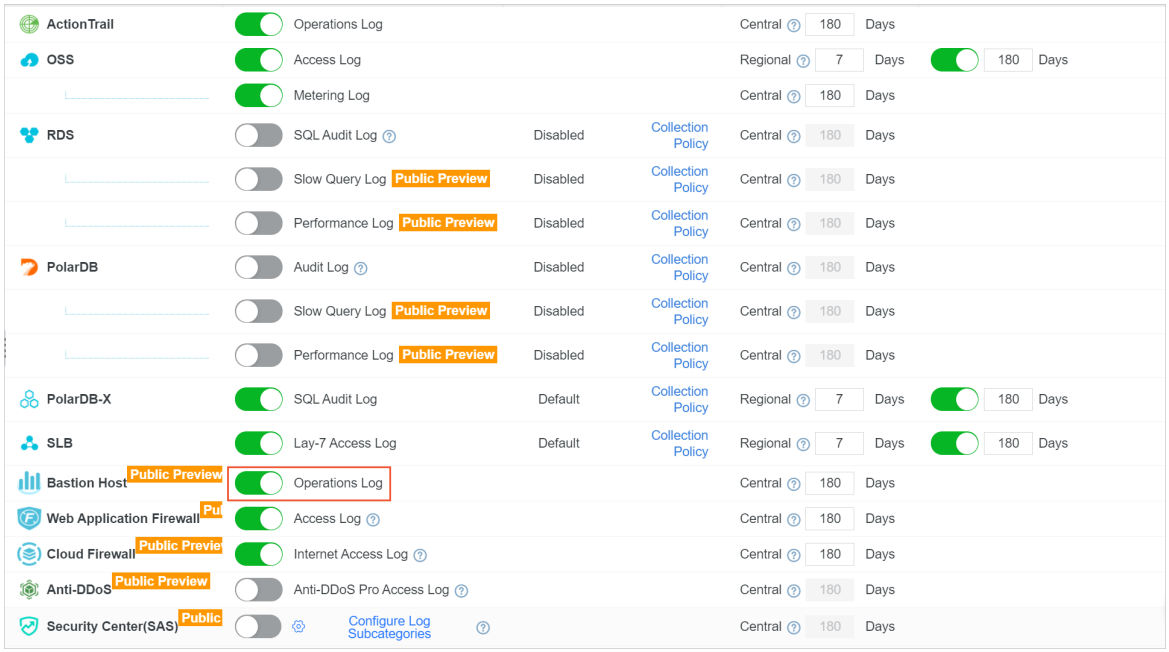
1. If Log Service is not activated, log on to the Log Service console and activate Log Service as prompted.
2. In the **Log Application** section, click **Log Audit Service**.
3. On the **Global Configurations** tab, complete the settings for collecting O&M logs.
   i. In the **Region of the Central Project** drop-down list, select a region for centralized storage of logs.
   ii. Authorize Log Service to collect and synchronize the O&M logs from Bastionhost.

   You can select manual authorization or AccessKey pair-based authorization. You can configure authorization for log collection by using one of the following methods:

   - **AccessKey Pair-Based Authorization**: Enter the AccessKey ID and AccessKey secret of an authorized Resource Access Management (RAM) user.

     The AccessKey pair is for temporary use and is not saved. The RAM user must have read and write permissions on RAM. For example, the RAM user is 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 O&M logs in the **Storage Type** column.



4. (Optional)View the O&M logs of Bastionhost.

   i. On the left-side navigation submenu, click the icon.

   ii. In the left-side navigation pane, click **Bastion Host** under **Central**.

   iii. On the **bastion_log** tab, view the O&M logs.

How do I allow the egress IP addresses of a bastion host in a security group of an ECS instance?

Before you use a bastion host to perform O&M operations on an ECS instance, you must create a security group rule for the ECS instance to allow the egress IP addresses of the bastion host. After you create a security group rule for the ECS instance to allow the egress IP addresses of the bastion host, the bastion host can communicate with the ECS instance. Then, you can use the bastion host to perform O&M operations on the ECS instance. You can perform the following steps to create the security group rule:

1. Log on to the Bastionhost console.
2. Find the bastion host that you want to use to perform O&M operations and move the pointer over the **Egress IP**.
3. Copy and save the public and private IP addresses of the bastion host.
4. Create a security group rule for the ECS instance to allow the public and private IP addresses.

   For more information about how to create a security group rule, see Add a security group rule.

How do I access an ECS instance from my bastion host by using an internal IP address?

You can use one of the following methods:

- Import an ECS instance. By default, you can access the ECS instance by using an internal IP address. For more information, see Import ECS instances.
- In the left-side navigation pane of the console of your bastion host, choose **Assets > Hosts**. On the Hosts page, select the host whose O&M IP address you want to change and choose **Batch > Modify O&M IP Address**. In the **Modify O&M IP Address** dialog box, set **Host IP Address Type** to **Private IP Address** and click **OK**.

How do I configure my bastion host if I want to access an ECS instance by using a port other than the SSH- or RDP-compliant standard port?

Bastion hosts support custom O&M ports. You can perform the following steps to specify a port in Bastionhost: In the left-side navigation pane of the console of your bastion host, choose **Assets > Hosts**. On the Hosts page, select the host whose O&M ports you want to change and choose **Batch > Modify O&M Port**. In the **Modify O&M Port** dialog box, specify the Protocol and Port parameters and click **OK**.

How long can audit videos in a bastion host be stored?

Audit videos for a bastion host that runs V3.2 can be stored for more than half a year in Object Storage Service (OSS). When the storage space for Bastionhost is about to reach the upper limit, the earliest audit logs and videos are automatically cleared.

> **Note** 云盾堡垒机实例直接保存运维协议的原始数据，根据流量不同所占用的空间大小也不同。

- SSH运维会话一般每天产生2 M左右日志数据。
- 远程桌面（RDP）运维会话（1024 * 768分辨率）一般每小时产生10 M左右日志数据。

If I use an RDP-based client, how do I switch to another host to perform O&M operations?

If you use an RDP-based client, perform the following steps to switch to another host to perform O&M operations:

1. Click the **Start** icon in the lower-left corner of your desktop.
2. In the **Start** menu, click the **Power** icon.
3. In the menu that appears, click **Disconnect**.
4. In the host list, select the host on which you want to perform O&M operations and log on to the host.

How do I configure a server as an HTTP or SOCKS5 proxy server?

In this example, an ECS instance that runs CentOS 8.3 is used to describe how to configure a server as an HTTP or SOCKS5 proxy server.

> **Note**
>
> - Before you configure a proxy server, make sure that the network between your bastion host and the proxy server is connected.
> - You can use Linux servers as SSH proxy servers without the need to install components or make configurations on the Linux servers.

1. Log on to the proxy server.
2. Run the **yum install 3proxy** command to install 3proxy.
3. Run the **vim /etc/3proxy.cfg** command to modify the configuration file.
   - Configure the username and password of the proxy server.

     ```
     users 3APA3A:CL:3apa3a "test:CR:$1$qwer$CHFTUFGqkjue9HyhcMHEe1" ceshi:CL:1qaz@WSX
     # note that "" required, overvise $... is treated as include file name.
     # $1$qwer$CHFTUFGqkjue9HyhcMHEe1 is 'test' in MD5 crypt format.
     #users $/usr/local/etc/3proxy/passwd
     # this example shows you how to include passwd file. For included files
     # <CR> and <LF> are treated as field separators.
     ```

   - Configure access control parameters.

     ```
     # for different clients.
     allow ceshi
     ```

   - Enable HTTP and SOCKS5 proxies and specify the listening port and the source IP address that is used to access the proxy server.

     ```
     auth strong
     # We want to protect internal interface
     deny * * 127.0.[redacted].,192.168.[redacted]
     # and llow HTTP and HTTPS traffic.
     allow * * * 80-88,8080-8088 HTTP
     allow * * * 443,8443 HTTPS
     proxy -i0.0.0.0 -p8080
     socks -i0.0.0.0 -p1080
     flush
     ```

4. Run the **bin/systemctl start 3proxy.service** command to enable the proxies.
5. Run the **iptables -F** command to disable the firewall of the server to ensure that the server can be accessed.
6. Create a security group rule for the server. For more information, see Add a security group rule.

   > **Note** When you create a security group rule, set Port Range to the listening port that is specified in Step 3 and Authorization Object to the egress IP addresses of your bastion host. To obtain the egress IP addresses, find your bastion host on the Instances page of the Bastionhost console and click **Egress IP**.

   After you create the security group rule for the server, the proxy server is configured.