

Alibaba Cloud

Bastion Host Product Introduction

Document Version: 20220617

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 .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.What is Bastionhost?	05
2.Functions and features	07
3.Benefits	10
4.Common scenarios	12
5.Pre-sales FAQ	14
6.Terms	22
7.Services that work with Bastionhost	24

1. What is Bastionhost?

Bastionhost is a system O&M and security audit platform provided by Alibaba Cloud. It allows you to centrally manage asset permissions and O&M operations, and play back recordings of O&M operations. This way, you can identify the users who perform specific O&M operations in the cloud, manage permissions, and audit O&M operations. Bastionhost makes asset management efficient, O&M responsibilities clear, and O&M events traceable. Bastionhost helps enterprises meet the requirements for classified protection.

Benefits

Bastionhost provides the following benefits:

- **Unified portal for O&M**

Bastionhost provides a unified portal for you to manage different accounts. You can use single sign-on (SSO) to access a large number of server resources in the backend. This improves O&M efficiency and prevents risks, such as passwords are forgotten or leaked.

- **Two-factor authentication**

Bastionhost provides the two-factor authentication feature. You can use a verification code in a multi-factor authentication (MFA) device or a verification code sent in a text message for identity authentication. This prevents unauthorized users from accessing assets by using leaked accounts and passwords.

- **Fine-grained permission assignment**

Bastionhost allows you to group users and assign permissions to the users at a fine granularity. You can control permissions such as file upload, download, and creation permissions. This helps implement flexible access control based on the principle of least privilege.

- **Automatic blocking of high-risk commands**

Bastionhost automatically blocks the running of high-risk commands, such as `rm -rf /*` (the command to delete data), and commands to format system disks. This helps prevent accidental deletion operations that may cause serious consequences.

- **Visualized audit for event tracing**

Bastionhost visualizes audit records. It records O&M sessions and allows you to play back the recordings. This way, you can collect evidence and trace security events in an efficient manner.

Editions

Bastionhost has the Basic Edition and HA Edition to meet the requirements of different users.

- **Basic Edition**

Bastionhost Basic Edition provides basic features, including two-factor authentication, O&M authorization, high-risk command blocking, and O&M audit. These features help small- and medium-sized enterprises ensure basic O&M security and meet the requirements of classified protection.

- **HA Edition**

Bastionhost HA Edition is suitable for the large-sized enterprises or enterprises in the sectors that have high requirements for O&M security, such as the public service, finance, gaming, online education, and technology development sectors.

Bastionhost HA Edition supports the O&M features that are provided by the Basic Edition. Bastionhost HA Edition also provides the following features to meet higher requirements for business O&M security:

- Higher business stability. Bastionhost HA Edition uses a dual-engine architecture. Both engines are active, which offers a Service Level Agreement (SLA) of 99.95%.
- Higher processing performance. Bastionhost HA Edition can maintain up to 10,000 hosts. However, Bastionhost Basic Edition can maintain up to 500 hosts.
- More O&M capabilities. For example, Bastionhost HA Edition allows you to perform O&M operations by using a web terminal and supports automatic password change. You can use automatic password change to regularly rotate passwords, which improves password security.
- More bandwidth and storage. Bastionhost HA Edition offers you better O&M experience.

For more information about the differences between Bastionhost Basic Edition and Bastionhost HA Edition, see [Functions and features](#).

2.Functions and features

Bastionhost is available in the Basic Edition and HA Edition. This topic describes the differences between these editions.


Background information

Bastionhost Basic Edition provides basic features, including two-factor authentication, O&M authorization, high-risk command blocking, and O&M audit. These features help small- and medium-sized enterprises ensure basic O&M security and meet the requirements of classified protection.

Bastionhost HA Edition is suitable for the large-sized enterprises or enterprises in the sectors that have high requirements for O&M security, such as the public service, finance, gaming, online education, and technology development sectors. Bastionhost HA Edition supports the O&M features that are provided by the Basic Edition. Bastionhost HA Edition also provides the following features to meet higher requirements for business O&M security:

- Higher business stability. Bastionhost HA Edition uses a dual-engine architecture. Both engines are active, which offers a Service Level Agreement (SLA) of 99.95%.
- Higher processing performance. Bastionhost HA Edition can maintain up to 10,000 hosts. However, Bastionhost Basic Edition can maintain only up to 500 hosts.
- More O&M capabilities. For example, Bastionhost HA Edition allows you to perform O&M operations by using a web terminal and supports automatic password change. You can use automatic password change to regularly rotate passwords, which improves password security.
- More bandwidth and storage. Bastionhost HA Edition offers you better O&M experience.

Bastionhost features

 **Note** In the following table, a tick (√) indicates that a feature is supported and a cross (×) indicates that a feature is not supported.

Feature	Description	Basic Edition	HA Edition	References
Architecture	The dual-engine and high-availability architecture ensures business and monitoring stability.	×	√	Benefits
Auto scaling	You can increase bandwidth and storage based on your business requirements.	√	√	Billing
Deployment	You can deploy a bastion host outside China. You can switch between simplified Chinese, traditional Chinese, and English based on your business requirements. Two-factor authentication supports the mobile phone numbers provided by telecom carriers outside China.	√	√	Which countries and regions support the SMS-based two-factor authentication feature of Bastionhost?

Feature	Description	Basic Edition	HA Edition	References
User and asset management	You can assign multiple roles to users.	√	√	None
	You can synchronize users from Resource Access Management (RAM), Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and Azure Active Directory (Azure AD). You can also import multiple users from a file at a time.	√	√	管理用户
	You can manage Windows or Linux servers and use the following protocols for O&M: SSH, Remote Desktop Protocol (RDP), and SSH File Transfer Protocol (SFTP).	√	√	Add hosts
	You can import multiple hosts at a time. You can import Alibaba Cloud Elastic Compute Service (ECS) instances by using a file or with a few clicks.	√	√	Add hosts
	You can maintain ApsaraDB for MyBase dedicated clusters, servers that are deployed on the cloud, and servers in data centers.	√	√	None
	You can implement two-factor authentication in multiple regions. Email- and SMS-based two-factor authentication is supported.	√	√	Enable two-factor authentication
	You can verify logons to your bastion host based on dynamic verification codes on apps.	√	√	None
	You can manually change the password of a Linux host account or create an automatic password change task to change the password on a regular basis.	×	√	Use the automatic password change feature
	This feature allows you to log on to your bastion host by using a client, such as a Windows Remote Desktop, XShell, SecureCRT, or PuTTY client, to access graphical or character devices. This feature records O&M operations and allows you to play back the recordings.	√	√	RDP-based O&M and SSH-based O&M
	This feature allows you to log on to your bastion host by using a local SFTP client, such as WinSCP, Xftp, and SecureFX, to perform O&M operations.	√	√	Perform SFTP-based O&M

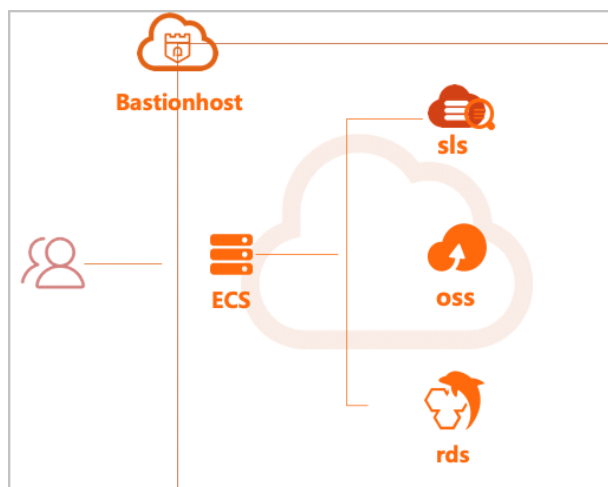
Feature	Description	Basic Edition	HA Edition	References
O&M management	This feature allows you to maintain servers on a web page.	×	√	Use the host O&M feature
	This feature monitors O&M sessions in real time and can block O&M sessions.	√	√	Search for real-time monitoring sessions and view session details and Interrupt sessions
	This feature controls the upload and download operations in the RDP clipboard, and mapping operations in RDP.	√	√	Create a control policy
	This feature allows you to block and approve important command policies.	√	√	
	This feature controls the following operations when you perform O&M operations by using a local SFTP client: upload, download, delete, and rename files, and create and delete folders.	√	√	
ActionTrail	This feature records operations logs and allows you to audit and play back the recordings.	√	√	None
	This feature allows you to audit the transfer of files.	√	√	
	This feature allows you to generate O&M reports and export O&M reports to PDF, HTML, or Word files.	√	√	O&M reports
API operation	This feature allows you to call API operations.	√	√	List of operations by function

3. Benefits

Bastionhost is built on top of a stable cloud architecture and runs in dual-engine mode. Bastionhost can be deployed across the globe to ensure stable, secure, and efficient O&M of assets. This topic describes the benefits of Bastionhost.

Stable cloud architecture

Bastionhost adopts a cloud architecture. Elastic Compute Service (ECS), Log Service, Object Storage Service (OSS), and ApsaraDB RDS, are independent of each other and the data of these services are separately stored. This prevents O&M interruptions caused by single points of failure (SPOFs). Log Service, OSS, and ApsaraDB RDS feature high performance and high maturity, and ensure the security of assets. Bastionhost that is built on top of the cloud architecture is more stable, flexible, and secure.



Secure and reliable O&M capability

Bastionhost allows you to perform efficient O&M on Linux operating systems. Bastionhost also allows you to run efficient and smooth O&M on Windows operating systems, and complete audit records are also provided. You can also perform centralized management and O&M on assets in hybrid clouds, which may involve different clouds, data centers, and virtual private clouds (VPCs). Bastionhost is a closed source service that can prevent attacks and ensure stable, secure O&M of assets.

Global deployment

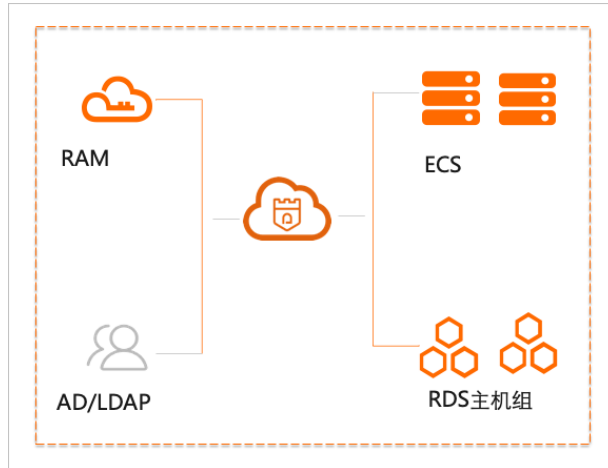
Bastionhost can be deployed across the globe, such as in regions in Asia Pacific, Americas, Europe, Middle East, and India. Bastionhost provides an English web UI and supports two-factor authentication by using mobile phone numbers in different countries. This ensures secure O&M of assets.

Dual-engine architecture

Bastion hosts run in dual-engine mode to ensure stable operation. In this mode, business workloads are balanced, and O&M efficiency is improved. If connection errors occur, the HA mode is automatically enabled to prevent service interruptions and ensure continuous monitoring.

Ease of use

Bastionhost can be used out of the box and is easy to use and upgrade. You can add ECS instances within your Alibaba Cloud account and hosts in dedicated clusters to bastion hosts with a few clicks. You can also import RAM users, Active Directory (AD) users, and Lightweight Directory Access Protocol (LDAP) users to bastion hosts with a few clicks. Bastionhost provides 24/7 remote support to meet your business requirements at any time.



4.Common scenarios

Bastionhost is used in various industries, such as the finance, education, public service sector, healthcare, media, and Internet industries. This topic describes the use of Bastionhost in different scenarios.

Finance

Challenges:

Financial institutions such as banks, securities firms, and insurance firms are crucial to social and economic development. Therefore, financial institutions must meet the strict regulatory requirements of security. The security of server assets within the enterprises is no exception. Financial institutions must strengthen the security monitoring of O&M operations on servers. The institutions must prevent data leaks that are caused by unauthorized access during O&M. The institutions must also prevent the breakdown of business systems caused by high-risk commands.

Solutions:

Bastionhost provides the following features to help financial institutions better monitor the O&M operations on servers:

- Prevention of unauthorized access

Bastionhost allows you to assign fine-grained permissions. This prevents data leaks caused by unauthorized access.

- Blocking of high-risk commands

Bastionhost blocks the running of high-risk commands in real time. This ensures the security of business systems during the O&M.

- Efficient recording playback

Bastionhost records O&M sessions and allows you to play back the recordings. This way, you can trace security events in an efficient manner.

Internet

Challenges:

The rapid development of the Internet industry has resulted in an increase in the number of employees and servers in Internet enterprises. Internet enterprises face issues such as disorganized access to server resources, difficult account management, and complex permission assignment.

Solutions:

Bastionhost provides the following features to help Internet enterprises better manage servers, user accounts, and permissions:

- Unified portal for O&M

Bastionhost provides a unified portal for you to manage different accounts. This allows you to access a large number of server resources in the backend.

- Account and password hosting

Bastionhost retains the usernames and passwords of hosts in a centralized manner. This allows you to log on to a host without the need to enter a password. This prevents security risks, such as difficulties in remembering different resource access accounts and passwords and password leaks.

- Fine-grained permission assignment

Bastionhost supports fine-grained flexible permission assignment to allow different users of Internet enterprises to perform operations based on the permissions that are assigned to these users. This helps implement access control based on the principle of least privilege. This also helps streamline permission management.

5.Pre-sales FAQ

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](#). Pre-sales 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?](#)
- [Can I synchronize ECS instances that reside in different VPCs to a bastion host?](#)
- [Can I use a single bastion host to perform O&M audit on the ECS instances that reside in different VPCs or regions or on the ECS instances that are deployed within different accounts?](#)
- [Am I charged for enabling SMS-based two-factor authentication?](#)
- [What is the operating system of bastion hosts? Can I replace this existing operating system with another operating system?](#)
- [Why are the available regions different when I purchase bastion hosts for different Alibaba Cloud accounts?](#)
- [Can bastion hosts be customized?](#)


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 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, bastion hosts have no control policies on IP addresses of Elastic Compute Service (ECS) instances. 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](#).


Can I synchronize ECS instances that reside in different VPCs to a bastion host?

The answer is based on whether the virtual private clouds (VPCs) belong to the same Alibaba Cloud account.

- If the VPCs belong to different Alibaba Cloud accounts, you cannot synchronize the ECS instances to a bastion host. We recommend that you deploy bastion hosts separately within each Alibaba Cloud account. You can also manually add ECS instances to your bastion host.

 **Note** If you want to perform O&M on ECS instances within different Alibaba Cloud accounts, make sure that the ECS instances are configured with public IP addresses. This way, you can access the ECS instances over the Internet from your bastion host.


- If the VPCs belong to the same Alibaba Cloud account, you can synchronize all the ECS instances to a bastion host.

 **Note** Before you perform O&M on the ECS instances that reside in different VPCs, make sure that you can access the ECS instances over an internal network by using Alibaba Cloud Express Connect or over the Internet from your bastion host.

Can I use a single bastion host to perform O&M audit on the ECS instances that reside in different VPCs or regions or on the ECS instances that are deployed within different accounts?

Yes, you can perform O&M audit on the ECS instances that reside in different VPCs or regions or are deployed within different accounts only if you can access the ECS instances from your bastion host.

- For example, you created more than 10 ECS instances within the same Alibaba Cloud account in three regions. If you can access these ECS instances from your bastion host, you can perform O&M audits on these ECS instances.
- For example, you created 13 ECS instances within the same Alibaba Cloud account. Nine ECS instances reside in the classic network and the other four ECS instances reside in a VPC. If you can access all these ECS instances from your bastion host, you can perform O&M audits on these ECS instances.

 **Note** If you cannot access all these ECS instances from your bastion host, you may need to deploy multiple bastion hosts to perform O&M audits on different ECS instances.

You can use the following methods to enable communications between ECS instances and bastion hosts:

- If the ECS instances for which you want to perform O&M are accessible over the Internet, add rules that allow access from the bastion hosts in the security groups of the ECS instances. For more information, see [Add a security group rule](#).
- If the ECS instances for which you want to perform O&M are deployed in a VPC, connect this VPC to bastion hosts by using a Cloud Enterprise Network (CEN). For more information, see [What is CEN?](#).

Am I charged for enabling SMS-based two-factor authentication?

No, you are not charged for enabling SMS-based two-factor authentication. For more information about how to enable SMS-based two-factor authentication, see [Enable two-factor authentication](#).

What is the operating system of bastion hosts? Can I replace this existing operating system with another operating system?


No, you cannot replace the operating system of bastion hosts. All bastion hosts run the CentOS operating system.

Why are the available regions different when I purchase bastion hosts for different Alibaba Cloud accounts?

Servers within different Alibaba Cloud account types implement physical isolation and network isolation. You can purchase bastion hosts in specific regions based on your account types, such as Alibaba Gov Cloud and Alibaba Finance Cloud accounts. For example, you can use only an Alibaba Gov Cloud account to purchase the bastion hosts deployed in the **China North 2 Ali Gov 1** region. You can go to the [buy page of Bastionhost](#) of Bastionhost to view the available regions for your account.

Can bastion hosts be customized?

No, you can select only the specifications that are offered by Alibaba Cloud. The following table describes the available specifications. For more information, see [Billing](#).

 **Note** Region 1, Region 2, and Region 3 in the following table refer to the following specific regions:

- **Region 1:** China (Hong Kong), Singapore (Singapore), Australia (Sydney), Malaysia (Kuala Lumpur), Indonesia (Jakarta), Japan (Tokyo), Germany (Frankfurt), UK (London), US (Virginia), US (Silicon Valley), and India (Mumbai)
- **Region 2:** China (Shanghai), China (Shenzhen), China (Qingdao), China (Beijing), China (Hohhot), and China (Chengdu)
- **Region 3:** UAE (Dubai)

Billable item		Specification	Maximum number of concurrent sessions	Service specification	Price in Region 1	Price in Region 2	Price in Region 3
		50 assets	50 <ul style="list-style-type: none"> • SSH-based O&M sessions only: 50 • RDP-based O&M sessions only: 20 		USD 400 per month	USD 250 per month	USD 750 per month

Billable item		Specification	Maximum number of concurrent sessions	Service specification	Price in Region 1	Price in Region 2	Price in Region 3
		100 assets	100 • SSH-based O&M sessions only: 100 • RDP-based O&M sessions only: 30	<ul style="list-style-type: none"> • Bandwidth: 1 Mbit/s • Storage: 1 TB 	USD 600 per month	USD 400 per month	USD 1,000 per month
		200 assets	100 • SSH-based O&M sessions only: 100 • RDP-based O&M sessions only: 30		USD 700 per month	USD 550 per month	USD 1,300 per month
		500 assets	500 • SSH-based O&M sessions only: 500 • RDP-based O&M sessions only: 60	<ul style="list-style-type: none"> • Bandwidth: 16 Mbit/s • Storage: 2 TB 	USD 1,100 per month	USD 800 per month	USD 2,000 per month

Billable item		Specification	Maximum number of concurrent sessions	Service specification	Price in Region 1	Price in Region 2	Price in Region 3
Basic fee		50 assets	50 <ul style="list-style-type: none"> SSH-based O&M sessions only: 50 RDP-based O&M sessions only: 50 	<ul style="list-style-type: none"> Bandwidth: 12 Mbit/s Storage: 2 TB 	USD 700 per month	USD 400 per month	N/A
		100 assets	100 <ul style="list-style-type: none"> SSH-based O&M sessions only: 100 RDP-based O&M sessions only: 60 		USD 1,000 per month	USD 700 per month	N/A
		200 assets	100 <ul style="list-style-type: none"> SSH-based O&M sessions only: 100 RDP-based O&M sessions only: 60 		USD 1,300 per month	USD 950 per month	N/A

Billable item		Specification	Maximum number of concurrent sessions	Service specification	Price in Region 1	Price in Region 2	Price in Region 3
		500 assets	500 <ul style="list-style-type: none"> SSH-based O&M sessions only: 500 RDP-based O&M sessions only: 120 	<ul style="list-style-type: none"> Bandwidth: 24 Mbit/s Storage: 3 TB 	USD 1,900 per month	USD 1,400 per month	N/A
		1,000 assets	1,000 <ul style="list-style-type: none"> SSH-based O&M sessions only: 1000 RDP-based O&M sessions only: 120 		USD 3,900 per month	USD 2,500 per month	N/A
		2,000 assets	1,000 <ul style="list-style-type: none"> SSH-based O&M sessions only: 1000 RDP-based O&M sessions only: 120 		USD 6,000 per month	USD 4,000 per month	N/A

Billable item		Specification	Maximum number of concurrent sessions	Service specification	Price in Region 1	Price in Region 2	Price in Region 3
		5,000 assets	2,000 <ul style="list-style-type: none"> SSH-based O&M sessions only: 2000 RDP-based O&M sessions only: 240 	<ul style="list-style-type: none"> Bandwidth: 48 Mbit/s Storage: 4 TB 	USD 8,800 per month	USD 5,800 per month	N/A
Extra bandwidth		Increment: 10 Mbit/s	N/A		N/A	USD 15 per Mbit/s per month	USD 12 per Mbit/s per month

Which countries and regions support the SMS-based two-factor authentication feature of Bastionhost?

The following table lists the countries and regions that support the text message-based two-factor authentication feature of Bastionhost.

Location	Country or special administrative region: country calling code
China	Hong Kong (China): +852
	Macau (China): +853
	Taiwan (China): +886
	Chinese mainland: +86
	Australia: +61
	Poland: +48
	Germany: +49
	Dubai: +971
	Russia: +7
	France: +33
	Philippines: +63


Location	Country or special administrative region: country calling code
Outside China	South Korea: +82
	Malaysia: +60
	US: +1
	Japan: +81
	Sweden: +46
	Switzerland: +41
	Spain: +34
	Singapore: +65
	Israel: +972
	Italy: +39
	India: +91
	Indonesia: +62
	UK: +44

6. Terms

This topic introduces the basic concepts related to Bastionhost.

Bastionhost administrator

A user who has full permissions on Bastionhost. The permissions of a Bastionhost administrator include asset management, user management, authorization rule management, control policy management, command approval, session auditing, host operation and management, and system settings.


 **Note** A Resource Access Management (RAM) user must be created before you can grant the Bastionhost administrative rights to the RAM user. For more information about how to create a RAM user, see [Create a RAM user](#).

Bastionhost O&M administrator

A user who has the permissions to log on to a bastion host and perform O&M operations on assets.


Bastionhost auditor

A user who has the permissions to view Bastionhost audit data. A Bastionhost auditor can block real-time sessions.

 **Note** A RAM user must be created before you can grant the Bastionhost auditor permissions to the RAM user. For more information about how to create a RAM user, see [Create a RAM user](#).

Bastionhost read-only permissions

The permissions to view all the features and configurations of Bastionhost. Users who have read-only permissions can only view the features and configurations of Bastionhost but cannot modify the features and configurations.

 **Note** A RAM user must be created before you can grant the Bastionhost read-only permissions to the RAM user. For more information about how to create a RAM user, see [Create a RAM user](#).

number of assets

The number of assets managed by a bastion host.

concurrency

The number of O&M sessions that are established on Bastionhost at the same time. For example, if 10 users simultaneously use Bastionhost to perform O&M operations on their assets and each user establishes five connections on average by using protocols, such as SSH and Remote Desktop Protocol (RDP), the concurrency is 50.

Client/Server O&M

A user uses an RDP or SSH client, such as Remote Desktop Connection (MSTSC) or Xshell, and enters the required information to log on to a bastion host and perform O&M operations on authorized assets. The information includes the username, password, O&M URL, and port number of the bastion host.

web terminal-based O&M

A RAM user is used to perform O&M operations on the authorized assets on a web page.

real-time monitoring


Real-time video recording of O&M operations that happen during a session.

session audit

Video playback of O&M operations that happen during a session.

credential hosting

Credentials are the passwords or keys of the accounts that are created for hosts. Credential hosting indicates that an administrator manages the passwords or keys of host accounts in Bastionhost.


 **Note** If a user wants to use Bastionhost to perform O&M operations on a host after the administrator authorizes the hosted credentials to the user, the user can directly log on to the host by using the credentials hosted on Bastionhost.

host fingerprint

A unique identifier that Bastionhost uses to identify a Linux host.

public key of a user

A public key in a key pair. Private and public keys are used for asymmetric encryption. A public key and a private key compose a key pair. A public key is used to encrypt data and is published by the owner of a key pair to users. Data that is encrypted by using the public key can be decrypted only by using the private key. A private key is used to decrypt the data that is encrypted by using the public key. It is owned by the owner of a key pair and cannot be published.

 **Note** A user can use a key pair to log on to a bastion host. After the public key is hosted on Bastionhost, the user can use the private key to log on to the bastion host.

network domain

LANs and virtual private clouds (VPCs) are network domains. If a network domain cannot communicate with the VPC in which your bastion host resides, you can specify a server in the network domain as a proxy server. Then, you can connect your bastion host to the proxy server to perform O&M operations on other servers in the network domain.

7.Services that work with Bastionhost

This topic describes the Alibaba Cloud services that can be used with Bastionhost.

Log Service

Bastionhost is connected to Log Service.

Bastionhost synchronizes logs to Log Service to provide the log analysis feature. This feature provides you with accurate and real-time log query and analysis. For more information, see [Archive audit logs in Log Service](#).

ActionTrail

Bastionhost is connected to ActionTrail.

ActionTrail is a service that monitors and records the actions of your Alibaba Cloud account. The actions include your access to and use of cloud services by using the Alibaba Cloud Management Console, APIs, and SDKs. ActionTrail records these actions as events. You can download these events from the ActionTrail console or configure ActionTrail to deliver these events to Log Service Logstores or Object Storage Service (OSS) buckets. Then, you can perform operations, such as action analysis, security analysis, resource change tracking, or compliance audit based on the events. For more information, see [What is ActionTrail?](#)

RAM

Bastionhost is connected to Resource Access Management (RAM).

RAM is a service provided by Alibaba Cloud to manage user identities and resource access permissions. RAM allows you to create and manage multiple identities for an Alibaba Cloud account, and grant different permissions to a single identity or a group of identities. This way, you can authorize different identities to access different Alibaba Cloud resources. For more information, see [What is RAM?](#)