ALIBABA CLOUD

Alibaba Cloud

Security Center
Defense

Document Version: 20220624

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.Anti-ransomware protection

1.1. Overview

Ransomware is one of the major threats to network security. Security Center provides a general anti-ransomware solution. The solution supports the features of anti-ransomware for servers and anti-ransomware for databases. This way, you can protect your servers and databases from ransomware.

Background information

Anti-ransomware is a value-added feature that is provided by Security Center. If you use the , , , or edition, you must purchase a specific amount of anti-ransomware capacity before you can use anti-ransomware to back up data. If you use the edition, you must upgrade Security Center to the , , , or edition or purchase the edition, and purchase a specific amount of anti-ransomware capacity before you can use the anti-ransomware feature.

How anti-ransomware works

Operating systems and versions supported by anti-ransomware for servers

Notice The following table lists operating systems and versions that are supported by anti-ransomware for servers. You can install the anti-ransomware agent only on the servers that run supported operating system versions. If your use other operating systems and versions, you cannot install the anti-ransomware agent or back up data. Before you use the anti-ransomware feature, we recommend that you check whether the operating system version of your server is supported.

Operating system	Supported version
Windows	7, 8, and 10
Windows Server	2008 R2, 2012, 2012 R2, 2016, and 2019
Red Hat Enterprise Linux (RHEL)	7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 7.8, 8, 8.1, and 8.2
CentOS	6.5, 6.9, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.2, and 8.3
Ubuntu	14.04, 16.04, 18.40, and 20.04
SUSE Linux Enterprise Server	11, 12, and 15

Database versions and operating system versions supported by anti-ransomware for databases

Notice The following table lists database versions and operating system versions that are supported by anti-ransomware for databases. You can install the anti-ransomware agent only on the following types of databases and operating system versions. If your use other types of databases or operating system versions, you cannot install the anti-ransomware agent or back up data. Before you use the anti-ransomware feature, we recommend that you check whether the versions of your database and operating system on your server are supported.

Database type	Supported database version	Supported operating system version
Oracle	9i	SUSE 9.3, RHEL 4, RHEL 5, SLES 9, and CentOS 4.5
	10g	RHEL 9, RHEL 4, RHEL 5, CentOS 4.6, SUSE 11 SP4, and RHEL 6.5
	11g	RHEL 5, RHEL 6, CentOS 6.4, RHEL 6.5, CentOS 6.5, Oracle Enterprise Linux 6.7, RHEL 7, Windows Server 2008 R2, Windows Server 2012 R2, and RHEL 6.0
	12c	Windows Server 2008 R2, RHEL 6.5, RHEL 6.5, and RHEL 7.5
	18c	RHEL 7.0 and Windows Server 2008 R2
	19c	Oracle Enterprise Linux 7.0
Oracle RAC	9i	SUSE 9.3 and RHEL
	10g	RHEL 5 and Windows Server 2008 R2
	11g	Windows Server 2008 R2, RHEL 5, Oracle Enterprise Linux 6.4, RHEL 6.5, and iSoft Server OS V3.0
	12c	CentOS 6, RHEL 6.5, Windows Server 2008 R2, CentOS 6.7, and Oracle Enterprise Linux 6
	18c	Windows Server 2008 R2
	19c	RHEL 7.6
Oracle Data Guard	11g	CentOS 6.4, CentOS 6.5, RHEL 6, and Windows Server 2008 R2
	12c	Oracle Enterprise Linux 6
MySQL	5.0	RHEL 5.0, RHEL 6.0, RHEL 6.5, Ubuntu 12.10, SLES 10, SUSE 11 SP4, Ubuntu 11.10, and Neokylin 6.0
	5.1	RHEL 6.5, SUSE 11 SP4, RHEL 6.5, and RHEL 6.0
	5.4	RHEL 6.5 and SUSE 11 SP4
	5.5	Ubuntu 12.04, Ubuntu 14.04, Debian 7.8, Debian 8.3, CentOS 6.0, and RHEL 6.5
	5.6	RHEL 5.0, RHEL 6.0, RHEL 6.5, Ubuntu 14.04, CentOS 6.0, and CentOS 7.2
	5.7	RHEL 6.0, RHEL 7.0, CentOS 7.0, RHEL 6.5, Ubuntu 16.04, CentOS 7.2, RHEL 7.0, and NeoKylin 7.0

Database type	Supported database version	Supported operating system version
	8.0	CentOS 6.7, RHEL 6.5, and CentOS 7.0
Microsoft SQL Server	2005	Windows Server 2008 R2 Service Pack 1
	2008	Windows Server 2008 R2 and Windows Server 2008 R2 Service Pack 1
	2008 R2	Windows Server 2008 R2
	2012	Windows Server 2012 RC
	2014	Windows Server 2008 R2 Service Pack 1 and Windows Server 2016
	2016 (RTM)	Windows Server 2012 R2
	2017	Windows Server 2012 and Windows Server 2016
	2019	Windows Server 2016
SQL Server AlwaysOn	2012, 2016, and 2017	Windows Server 2012 R2

1.2. Enable anti-ransomware

To use the anti-ransomware feature of Security Center, you must purchase and enable the feature.

Context

If this is the first time that you use the anti-ransomware feature, you must assign the following roles to your Alibaba Cloud account: AliyunHBRDefaultRole and AliyunECSAccessingHBRRole.

Notice The anti-ransomware agent supports a limited number of operating system versions. You cannot install the anti-ransomware agent on or back up data for servers that run unsupported operating system versions. For more information about the supported operating system versions, see Operating systems and versions supported by anti-ransomware for servers and Database versions and operating system versions supported by anti-ransomware for databases. Before you purchase a specific amount of anti-ransomware capacity, make sure that your servers run supported operating system versions.

Limits

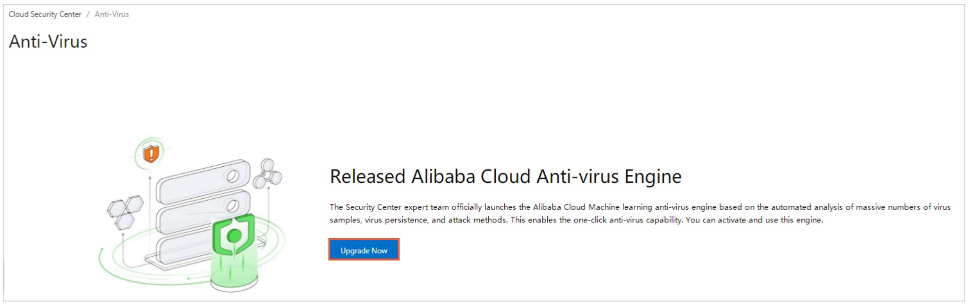
Anti-ransomware is a value-added feature that is provided by Security Center. If you use the , , , or edition, you must purchase a specific amount of anti-ransomware capacity before you can use anti-ransomware to back up data. If you use the edition, you must upgrade Security Center to the , , , or edition or purchase the edition, and purchase a specific amount of anti-ransomware capacity before you can use the anti-ransomware feature.

Procedure

1.

2.
3. On the **Anti-blackmail** page, click **Authorize**.
4. On the **Cloud Resource Access Authorization** page, click **Confirm Authorization Policy**.

   To use the anti-ransomware feature, you must assign the following roles to your account: AliyunHBRDefaultRole and AliyunECSAccessingHBRRole.
5. Click **Upgrade Now**.

   Released Alibaba Cloud Anti-virus Engine

   The Security Center expert team officially launches the Alibaba Cloud Machine learning anti-virus engine based on the automated analysis of massive numbers of virus samples, virus persistence, and attack methods. This enables the one-click anti-virus capability. You can activate and use this engine.
6. In the **Select a product version** panel, click **Upgrade**.
7. On the **Security Center buy page**, select an edition and specify the **Anti-ransomware** parameter.

   You can purchase an edition of Security Center based on your business requirements.

   - You can purchase the , , , , or edition. For more information about the features that each edition supports, see Features.
   - The anti-ransomware capacity is the storage capacity that can be used to store the backup data for your servers and databases. We recommend that you purchase anti-ransomware capacity based on the actual size of data that requires protection. If you cannot estimate the data size, we recommend that you purchase an anti-ransomware capacity of 50 GB for each server. For more information about the billing rules, see Billing.
8. Click **Buy Now** and complete the payment.

1.3. Enable anti-ransomware for servers

1.3.1. Create an anti-ransomware policy

Ransomware has become a major threat to cybersecurity. Security Center provides protection, generates alerts, and backs up data to protect your server from ransomware. You can create an anti-ransomware policy based on which data on your server is backed up. This topic describes how to create an anti-ransomware policy.

Prerequisites

A specific amount of anti-ransomware capacity is purchased. The permissions to use anti-ransomware are granted. For more information, see Enable anti-ransomware.

Context

You can use the anti-ransomware feature of Security Center to create anti-ransomware policies for your server. The server can be an Elastic Compute Service (ECS) instance, a server that is not deployed on Alibaba Cloud, a server that is deployed in the classic network, or a server that is deployed in a virtual

private cloud (VPC). After you create an anti-ransomware policy, Security Center automatically backs up data in protected directories on your server. If your server is attacked by ransomware, you can restore data based on the backups. This prevents negative impacts on your business.
The anti-ransomware agent that is installed on your server is used to back up data. You can back up data only if the agent is running properly. After you create an anti-ransomware policy, we recommend that you monitor the status of the anti-ransomware agent and handle the exceptions on the agent in a timely manner. For more information, see View the status of the anti-ransomware agent.

Limits

Version description

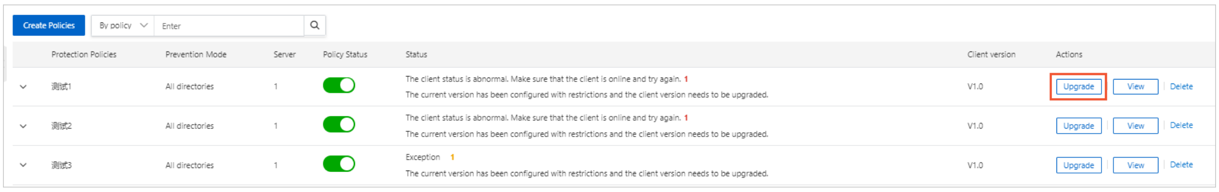
The version of the anti-ransomware agent is upgraded to V2.0 or later. You can no longer modify the existing V1.0 anti-ransomware policies based on which the V1.X.X anti-ransomware agent is installed. After the agent upgrade, you can create only V2.0 anti-ransomware policies.

The following table describes the differences between a V1.0 anti-ransomware policy and a V2.0 anti-ransomware policy.

Item	V1.0 anti-ransomware policy	V2.0 anti-ransomware policy
Custom directories to be excluded	Not supported.	Supported.
VSS		
Classic network		
Compatibility with Hybrid Backup Recovery (HBR)		
Backup method	Multiple data backup tasks can be run at a time, which may cause high CPU utilization.	Multiple data backup tasks can be run in sequence.

Upgrade V1.0 anti-ransomware policies with a few clicks

You can upgrade a V1.0 anti-ransomware policy to a V2.0 anti-ransomware policy with a few clicks. To upgrade a V1.0 anti-ransomware policy, you can click **Upgrade** in the **Actions** column on the Server extortion virus protection tab of the General Anti-ransomware Solutions page. During the policy upgrade, the version of the anti-ransomware agent that is installed based on the anti-ransomware policy is automatically upgraded to V2.X.X.



	Protection Policies	Prevention Mode	Server	Policy Status	Status	Client version	Actions
⌄	测试1	All directories	1	●	The client status is abnormal. Make sure that the client is online and try again. 1 The current version has been configured with restrictions and the client version needs to be upgraded.	V1.0	Upgrade | View | Delete
⌄	测试2	All directories	1	●	The client status is abnormal. Make sure that the client is online and try again. 1 The current version has been configured with restrictions and the client version needs to be upgraded.	V1.0	Upgrade | View | Delete
⌄	测试3	All directories	1	●	Exception 1 The current version has been configured with restrictions and the client version needs to be upgraded.	V1.0	Upgrade | View | Delete

Note

- The upgrade of the anti-ransomware agent does not affect backup data. After the upgrade, your data backup tasks run as expected. If the upgrade fails, the version of the anti-ransomware agent is automatically rolled back to V1.X.X, and data backup tasks are not affected.
- For some servers, the installed anti-ransomware agent cannot be upgraded with a few clicks. In this case, we recommend that you remove the server on which the anti-ransomware agent fails to be upgraded from the anti-ransomware policy, and click **Upgrade** in the **Actions** column for the anti-ransomware policy to upgrade the policy. After the anti-ransomware policy is upgraded, reapply the anti-ransomware policy to the server that you remove. Then, the V2.X.X anti-ransomware agent is automatically installed on the server.

Data backup

- You can incrementally back up data to protect your server against ransomware. If this is the first time that you back up all data in protected directories based on an anti-ransomware policy, a large number of CPU and memory resources are consumed. To avoid impacts on your services, we recommend that you back up data during off-peak hours. In subsequent backups, Security Center backs up only files that are newly added, modified, or deleted. This reduces server resource consumption and prevents excessive consumption of the anti-ransomware capacity.
- Security Center starts a specific number of data backup tasks based on the versions of anti-ransomware policies and the directories that you want to back up.

Directory to back up	V1.0 anti-ransomware policy	V2.0 anti-ransomware policy
All directories	○ For a Linux server, Security Center generates only one data backup task. ○ For a Windows server, Security Center generates one data backup task for each data disk. If your Windows server has two data disks, Security Center generates two data backup tasks. The two tasks start at the same time. Compared with a Linux server, the Windows server consumes more CPU and memory resources during backup. **Notice** We recommend that you schedule the data backup tasks based on the CPU utilization and memory usage of your Windows server.	For a server, Security Center generates only one data backup task. For multiple servers, Security Center generates multiple data backup tasks and

Directory to back up	V1.0 anti-ransomware policy	V2.0 anti-ransomware policy
Specific directories	Security Center starts one data backup task for each directory that is specified in an anti-ransomware policy. Security Center allows multiple data backup tasks to run at the same time. The tasks may consume a large number of CPU and memory resources. **Notice** We recommend that you specify an appropriate number of directories in the anti-ransomware policy based on your business requirements.	starts the tasks in sequence. This consumes less CPU and memory resources and does not affect your services.

Create an anti-ransomware policy

You can select **Recommendation Policy** to use the recommended anti-ransomware policy. You can also select **Custom policy** to create a custom anti-ransomware policy. To create an anti-ransomware policy based on which the V2.X.X anti-ransomware agent is installed, perform the following steps:

1.
2.
3.
4.
5. In the **Create Policies** panel, configure the parameters.

   The following table describes the parameters.

Parameter	Description
Policy Name	The name of the anti-ransomware policy.
Server Type	The type of the server to which you want to apply the anti-ransomware policy.

Parameter	Description
Select Assets	The assets that you want to protect. You can select an asset, an asset group, or multiple assets from asset groups. To select the assets that you want to protect, perform the following operations: ○ In the **Asset Group** section, select an asset group. Then, all assets in the group are selected. You can clear assets that do not require protection in the **Assets** section. ○ In the **Assets** section, enter the name of an asset in the search box to search for the asset. Fuzzy match is supported. ? **Note** ○ If you want to apply the anti-ransomware policy to ECS instances, you can select ECS instances that reside in different regions. If you want to apply the anti-ransomware policy to the servers that are not deployed on Alibaba Cloud, you must select the servers that reside in the same region. ○ To make sure that the anti-ransomware capacity is effectively utilized, you can add a server to only one policy.

Parameter	Description
Protection Policies	The anti-ransomware policy that you want to configure. Valid values: ○ **Recommendation Policy** If you select **Recommendation Policy**, the default values of the following parameters are used: ■ **Protected Directories**: All directories ■ **Directory to Exclude**: Excluded ■ **Exclude specified directories**: directories that are excluded from the policy ■ **Protected File Types**: All File Types ■ **Start Time**: a point in time within the range of 00:00 to 03:00 ■ **Backup policy execution interval**: One Day ■ **Backup data retention period**: 7 Days ■ **The bandwidth limit of the backup network**: 0 MByte/s **Note** The value 0 indicates that no limits are imposed on the bandwidth. ■ **VSS (Windows)**: Yes **Note** The VSS feature is available only if you create the anti-ransomware policy for Windows servers. After you enable the feature, the number of backup failures due to running processes is significantly reduced. We recommend that you enable the VSS feature. After you enable the feature, the data of disks that are in the exFAT and FAT32 formats cannot be backed up. ○ **Custom policy** If you select **Custom policy**, you must configure parameters based on your business requirements. The parameters include Protected Directories, Protected File Types, Start Time, Backup policy execution interval, Backup data retention period, and The bandwidth limit of the backup network.

Parameter	Description
Protected Directories	The directories that you want to back up. Valid values: - **Specified directory**: Security Center backs up only specified directories of the specified servers. Enter the addresses of the specified directories for **Protect directory address**. You can enter up to 20 addresses. - **All directories**: Security Center backs up all directories of the specified servers. You must set **Directory to Exclude** to **Not Exclude**. **Note** If you set Protected Directories to **All directories**, we recommend that you set **Directory to Exclude** to **Not Excluded**. This prevents system conflicts.
Directory to Exclude	Specifies whether to exclude system directories. If you set this parameter to **Excluded**, the system directories that are automatically specified for **Exclude specified directories** are excluded. You can also add or remove system directories based on your business requirements. **Note** System directories that are automatically excluded from the anti-ransomware policy for Windows and Linux servers are in update. You can view the system directories that are automatically excluded to the right of the **Exclude specified directories** parameter.
Protected File Types	The type of the files that you want to protect. Valid values: - **All File Types**: Security Center protects all files. - **Specify file type**: Security Center protects files only of the selected file type. Valid values: - **Document** - **Compressed** - **Database** - **Audio and video** - **Script code** **Notice** - If you set **Protected File Types** to **Specify file type**, you must select a file type from the drop-down list that appears. - You can select multiple file types. Security Center protects only the files of the selected file types.

Parameter	Description
Start Time	The time at which you want to start a data backup task. **Notice** If this is the first time that you back up all data in protected directories based on an anti-ransomware policy, a large number of CPU and memory resources are consumed. To avoid impacts on your services, we recommend that you back up data during off-peak hours.
Backup policy execution interval	The time interval between two data backup tasks. Default value: One Day. Valid values: - Half a day - One Day - 3 days - Seven Days
Backup data retention period	The retention period of backup data. Default value: 7 Days. **Notice** The backup data is stored only within the specified retention period. We recommend that you specify the retention period based on your business requirements. Valid values: - **Permanent** - **Custom** **Note** You can specify a retention period. Valid values: 1 to 65535. Unit: days.
The bandwidth limit of the backup network	The maximum bandwidth that can be consumed by a data backup task. Valid values: 1 to unlimited. Unit: MB/s. **Notice** If you create the anti-ransomware policy for an ECS instance, only internal network bandwidth is consumed. We recommend that you specify an appropriate bandwidth threshold based on the bandwidth of your server. This prevents the backup tasks from using an excessive amount of bandwidth and ensures service stability.

6. Click **Ok**.

   After the anti-ransomware policy is created, the policy is enabled by default, and Security Center installs the anti-ransomware agent on your server. Then, Security Center backs up data in the protected directories of your server based on the backup settings that you configure in the anti-ransomware policy.

What to do next

- View the status of the anti-ransomware agent

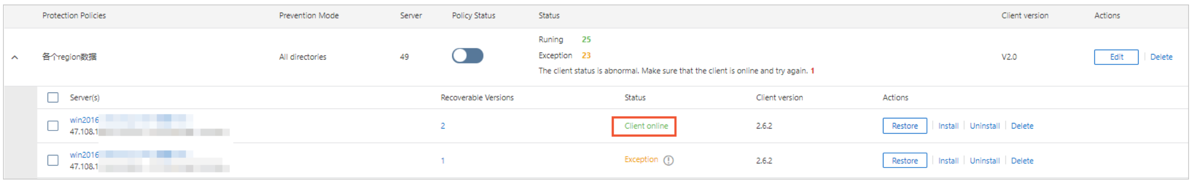
  After the anti-ransomware policy is created, you must check the status of the anti-ransomware agent that is installed on the servers protected by the anti-ransomware policy and make sure that the anti-ransomware agent is in the **Client online** state. To check the status of the anti-ransomware agent, go to the **Server extortion virus protection** tab of the Anti-blackmail page, find the anti-ransomware policy, and then click the ⌄ icon next to the policy name. In the list of servers that are protected by the anti-ransomware policy, view the agent status in the Status column. Security Center can back up data for the servers only if the anti-ransomware agent is in the **Client online** state.

  If the status of the anti-ransomware agent is **Not Installed**, **failed**, or **Exception**, data backup fails. You must identify the cause of the exception to the anti-ransomware agent and handle the exception.

  > **Note** If the status of the anti-ransomware agent is Exception, errors may occur during data backup or data restoration. If errors occur during data restoration, data backup tasks are not affected. You can handle the exception as prompted.

  You can use one of the following methods to handle the exception:

  - Follow the instructions on the Anti-blackmail page.
  - To contact Alibaba Cloud security engineers, .

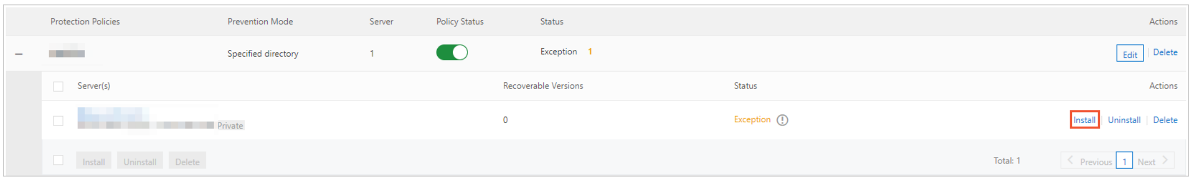


	Protection Policies	Prevention Mode	Server	Policy Status	Status	Client version	Actions
^	各个region数据	All directories	49		Runing 25 Exception 23 The client status is abnormal. Make sure that the client is online and try again. 1	V2.0	Edit | Delete

□	Server(s)	Recoverable Versions	Status	Client version	Actions
□	win2016[redacted] 47.108.1[redacted]	2	Client online	2.6.2	Restore | Install | Uninstall | Delete
□	win2016[redacted] 47.108.1[redacted]	1	Exception ⓘ	2.6.2	Restore | Install | Uninstall | Delete

- Manually install the anti-ransomware agent

  After the anti-ransomware policy is created, Security Center automatically installs the anti-ransomware agent on your server. If your server is not started or is configured with specific firewall policies, Security Center may fail to install the anti-ransomware agent on the server. If the anti-ransomware agent fails to be installed, you must identify the cause and resolve the issue. Then, install the anti-ransomware agent on the server. For more information about how to manually install the anti-ransomware agent, see Manage servers that are added to an anti-ransomware policy.



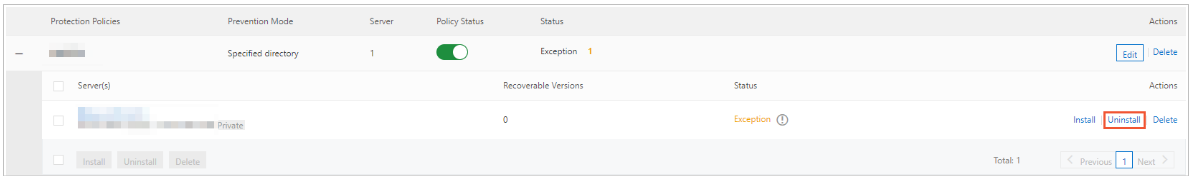
	Protection Policies	Prevention Mode	Server	Policy Status	Status	Actions
–	[redacted]	Specified directory	1		Exception 1	Edit | Delete

□	Server(s)	Recoverable Versions	Status	Actions
□	[redacted] Private	0	Exception ⓘ	Install | Uninstall | Delete
□	Install Uninstall Delete			Total: 1 ‹ Previous 1 Next ›

- Uninstall the anti-ransomware agent

  If the status of the anti-ransomware agent that is installed on the server in the anti-ransomware policy is **Exception** or **failed**, you can click **Uninstall** in the **Actions** column for the server to uninstall the anti-ransomware agent. Then, reinstall the anti-ransomware agent on the server.

> **Note** If you uninstall the anti-ransomware agent within the period specified by the **Backup data retention period** parameter, Security Center does not delete the data that the anti-ransomware agent backs up. If you uninstall the anti-ransomware agent in the time that is not within the period specified by the **Backup data retention period** parameter, Security Center deletes the backup data of the server.



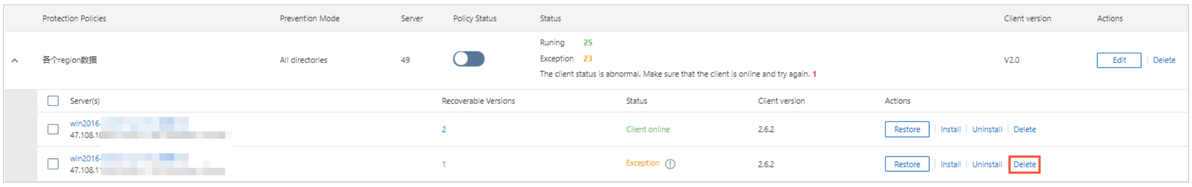
	Protection Policies	Prevention Mode	Server	Policy Status	Status	Actions
–	[redacted]	Specified directory	1	●	Exception 1	Edit | Delete

	Server(s)	Recoverable Versions	Status	Actions
□	[redacted] Private	0	Exception ⓘ	Install | Uninstall | Delete
□	Install Uninstall Delete		Total: 1	< Previous 1 Next >

- Delete the anti-ransomware agent

  If a server no longer requires the anti-ransomware policy, you can delete the anti-ransomware agent from the server. If you delete the anti-ransomware agent from the server, the server is deleted from the list of servers that use the anti-ransomware policy, and the backup data of the server is deleted. After the backup data on the server is deleted, Security Center releases the anti-ransomware capacity. The anti-ransomware capacity is updated within 24 to 72 hours after the release. We recommend that you do not run out of the anti-ransomware capacity. If the anti-ransomware capacity is used up, data backup tasks stop, and a full backup is performed. This significantly increases the resource usage of the server.

> **Notice** If the anti-ransomware agent is deleted from your server, the backup data on your server is also deleted. Deleted backup data cannot be recovered. Proceed with caution.



	Protection Policies	Prevention Mode	Server	Policy Status	Status	Client version	Actions
^	各个region数据	All directories	49	○	Runing 25 Exception 23 The client status is abnormal. Make sure that the client is online and try again. 1	V2.0	Edit | Delete

	Server(s)	Recoverable Versions	Status	Client version	Actions
□	win2016-[redacted] 47.108.1[redacted]	2	Client online	2.6.2	Restore | Install | Uninstall | Delete
□	win2016-[redacted] 47.108.1[redacted]	1	Exception ⓘ	2.6.2	Restore | Install | Uninstall | Delete

1.3.2. Manage an anti-ransomware policy

After you create an anti-ransomware policy, you can disable or enable it. You can also change the policy name and protected directory addresses, and manage the protected servers. If you no longer require the anti-ransomware policy, you can delete it. This topic describes how to disable, enable, edit, and delete an anti-ransomware policy. This topic also describes how to manage the servers that are added to an anti-ransomware policy.

Prerequisites

An anti-ransomware policy is created. For more information, see Create an anti-ransomware policy.

Context

An anti-ransomware policy takes effect only when the status of the anti-ransomware policy is **Normal**. If the status of the anti-ransomware policy is **Exception**, we recommend that you handle the exception at the earliest opportunity. For more information, see What do I do if the status of an anti-ransomware policy is abnormal?

Disable or enable an anti-ransomware policy

1.

2.

3.

4. On the **Server extortion virus protection** tab, find the anti-ransomware policy that you want to disable or enable and turn off or turn on the switch in the **Policy Status** column.
   - **Disable an anti-ransomware policy**
     If you back up the data on your server based on the anti-ransomware policy for the first time, a large number of CPU and memory resources may be consumed. As a result, your services may be affected. To prevent resource waste and service interruption, turn off the switch in the **Policy Status** column to disable the anti-ransomware policy. After you disable the anti-ransomware policy, the data backup task that is running based on the policy stops. We recommend that you enable the anti-ransomware policy during off-peak hours to back up data.
   - **Enable an anti-ransomware policy**
     By default, after you create an anti-ransomware policy for a server, the policy is enabled. If you disable the anti-ransomware policy because the data backup task consumes a large number of CPU and memory resources of your server, you can enable the policy during off-peak hours. The data on your server can be backed up based on the anti-ransomware policy only when the policy is enabled. To enable the policy, turn on the switch in the **Policy Status** column.

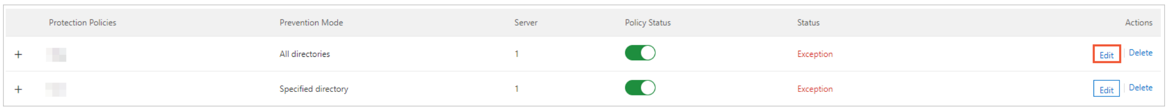
Edit an anti-ransomware policy

1.

2.

3.

4. On the **Server extortion virus protection** tab, find the anti-ransomware policy that you want to edit and click **Edit** in the Actions column.



	Protection Policies	Prevention Mode	Server	Policy Status	Status	Actions
+	[redacted]	All directories	1	●	Exception	Edit | Delete
+	[redacted]	Specified directory	1	●	Exception	Edit | Delete

5. In the **Edit Policies** panel, configure the parameters.

   For more information about the parameters, see Create an anti-ransomware policy.

6. Click **OK**.
   Security Center runs data backup tasks based on the anti-ransomware policy after modification.

Manage servers that are added to an anti-ransomware policy

After you create an anti-ransomware policy, you can add servers to or remove servers from the anti-ransomware policy. You can also install the anti-ransomware agent on your servers or uninstall the agent from your servers.

1.

2.

3.

4. On the **Server extortion virus protection** tab, find the anti-ransomware policy whose servers you want to manage and click the ⌄ icon. The servers to which the anti-ransomware policy is applied are displayed.

5. Manage the servers that are displayed.

   You can perform the following operations:

- **Add servers to the anti-ransomware policy**
  When you edit the anti-ransomware policy, you can add servers to the anti-ransomware policy. For more information, see Edit an anti-ransomware policy.

  > **Note** To make sure that the anti-ransomware capacity is effectively utilized, you can add a server to only one policy. You can add a maximum of 100 servers to each anti-ransomware policy.

- **Remove servers from the anti-ransomware policy**

  > **Notice** After a server is removed from the anti-ransomware policy, Security Center no longer protects the server against ransomware and deletes all backup data of the server. Deleted backup data cannot be restored. Proceed with caution.

  If you no longer require anti-ransomware for a server, click **Delete** in the Actions column. In the message that appears, click **OK**. If you want to remove multiple servers from an anti-ransomware policy, select the servers and click **Delete** below the server list.

- **Install or uninstall the anti-ransomware agent**
  If you want to install the anti-ransomware agent on a server or uninstall the anti-ransomware agent from a server, click **Install** or **Uninstall** in the Actions column. If you want to install the anti-ransomware agent on servers or uninstall the anti-ransomware agent from servers that are added to the same anti-ransomware policy, select the servers and click **Install** or **Uninstall** below the server list.

Delete an anti-ransomware policy

> **Notice** After you delete an anti-ransomware policy, the data backup task that is running based on the policy stops. In addition, the backup data of all servers on which the policy takes effect is deleted. Deleted backup data cannot be restored. Proceed with caution.

1.
2.
3.
4. On the **Server extortion virus protection** tab, find the anti-ransomware policy that you want to delete and click **Delete** in the Actions column.
5. In the **Are you sure you want to delete the current policy?** message, click **OK**.

1.3.3. Troubleshoot the issues causing the abnormal status of the anti-ransomware agent on your server

If you applied an anti-ransomware policy to your server and the status of the anti-ransomware agent is abnormal in the Security Center console, you can troubleshoot the issues that cause the abnormal status of the agent. This topic describes how to troubleshoot the issues.

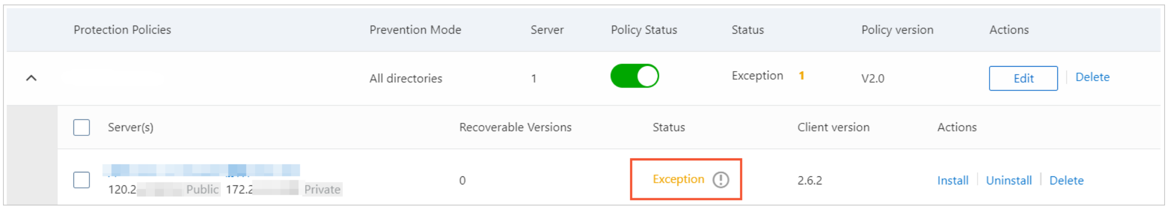
Context

If the status of the anti-ransomware agent is abnormal, the agent cannot back up the data on your server or protect your server. We recommend that you troubleshoot the issues that cause the abnormal status of the agent at the earliest opportunity.

Procedure

1.
2.
3. On the **Server extortion virus protection** tab, view the servers on which the anti-ransomware agent is in an abnormal state.

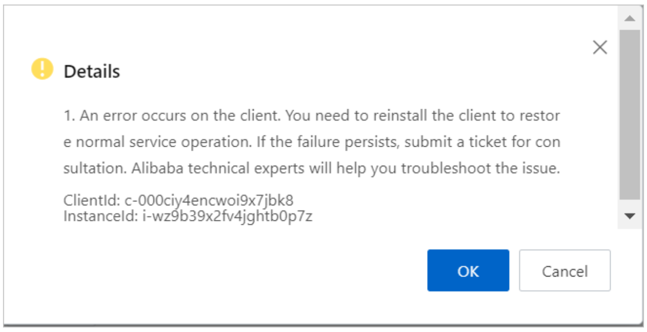
   Find an anti-ransomware policy and click the ⌄ icon next to the policy name to view all servers to which the policy is applied.



	Protection Policies	Prevention Mode	Server	Policy Status	Status	Policy version	Actions
^	[redacted]	All directories	1	●	Exception 1	V2.0	Edit | Delete

□	Server(s)	Recoverable Versions	Status	Client version	Actions
□	[redacted] 120.2[redacted] Public 172.2[redacted] Private	0	Exception ⓘ	2.6.2	Install | Uninstall | Delete

4. Find a server on which the anti-ransomware agent is in an abnormal state and click the ⓘ icon to view the causes of the status.



Details

1. An error occurs on the client. You need to reinstall the client to restore normal service operation. If the failure persists, submit a ticket for consultation. Alibaba technical experts will help you troubleshoot the issue.

ClientId: c-000ciy4encwoi9x7jbk8
InstanceId: i-wz9b39x2fv4jghtb0p7z

5. Troubleshoot the issues that cause the abnormal status based on the information in the **Details** message.

   For more information about the causes of the abnormal status for the anti-ransomware agent and how to troubleshoot the issues, see Causes of the abnormal status for the anti-ransomware agent and solutions.

Causes of the abnormal status for the anti-ransomware agent and solutions

Error code	Information in the Details message	Cause	Solution

Error code	Information in the Details message	Cause	Solution
CLOUD_ASSIST_NOT_RUN	Cloud assistant Not started	Cloud Assistant is not started.	Perform the following operations to troubleshoot the issues that are related to Cloud Assistant: 1. Log on to the ECS console. 2. Check whether Cloud Assistant is started. For more information, see Cloud Assistant troubleshooting FAQ. ○ If Cloud Assistant is not started, start the Cloud Assistant client. For more information, see Start or stop the Cloud Assistant client. ○ If Cloud Assistant is started, to address the issue.
RoleNotExist	Your Alibaba Cloud account is not authorized.	Your Alibaba Cloud account does not have the required permissions.	Log on to the Security Center console by using your Alibaba Cloud account. On the **Anti-blackmail** page, click the **Server extortion virus protection** tab. On the Server extortion virus protection tab, assign the **AliyunHBRDefaultRole** and **AliyunECSAccessingHBRRole** roles to your account.
CLIENT_CONNECTION_ERROR	The client connection is abnormal. Check the ECS instance network and try again.	The network connection fails.	Perform the following operations to troubleshoot network connection issues: 1. Log on to your ECS instance, run the `ping` or `telnet` command to test the connectivity between the ECS instance and the anti-ransomware endpoint, and then check whether firewall policies are configured for the ECS instance. For more information about anti-ransomware endpoints, see Anti-ransomware endpoints. 2. After you troubleshoot network connection issues, reinstall the anti-ransomware agent.

Error code	Information in the Details message	Cause	Solution
ECS_ROLE_POLICY_NOT_EXIST	ecs role does not have AliyunECSAccessingHBRRolePolicy	The AliyunECSAccessingHBRRolePolicy policy is not attached to the RAM role that your ECS instance assumes, which causes the failure to install the anti-ransomware agent.	Perform the following operations to troubleshoot issues: 1. Attach the AliyunECSAccessingHBRRolePolicy policy to the RAM role that your ECS instance assumes. For more information, see What can I do if the error message "The strategy of AliyunECSAccessingHBRRolePolicy is missing on EcsRamRole. Please refer to the FAQ for authorization" appears when I install the HBR backup client on an ECS instance?. 2. Reinstall the anti-ransomware agent. **Notice** After you attach the AliyunECSAccessingHBRRolePolicy policy to the RAM role that your ECS instance assumes, the anti-ransomware agent is not automatically installed on the ECS instance. You can log on to the Security Center console, go to the Anti-blackmail page, and manually install the anti-ransomware agent.
CHECK_ACTIVATION_COMMAND_TIMEOUT	The activation command times out.	The installation of the anti-ransomware agent times out.	Perform the following operations to reinstall the anti-ransomware agent: 1. Log on to the . On the Anti-blackmail page, click the **Server extortion virus protection** tab. On the Server extortion virus protection tab, uninstall the anti-ransomware agent. After you uninstall the anti-ransomware agent, the status of the agent changes to **Not Installed**. 2. Reinstall the anti-ransomware agent.
ECS_STOPPED	The ECS instance is not started.	The anti-ransomware agent fails to be installed because the ECS instance is not started.	Perform the following operations to start the ECS instance and then reinstall the anti-ransomware agent: 1. Log on to the ECS console. Start the ECS instance that is stopped. For more information, see Start an instance. 2. Reinstall the anti-ransomware agent.

Error code	Information in the Details message	Cause	Solution
UNINSTALL_FAILED	Failed to uninstall client	The anti-ransomware agent fails to be uninstalled because the execution of the Cloud Assistant command times out.	Perform the following operations to reinstall the anti-ransomware agent: 1. Log on to the . On the Anti-blackmail page, click the **Server extortion virus protection** tab. On the Server extortion virus protection tab, find an anti-ransomware policy that is applied to specific servers, select the server from which the anti-ransomware agent fails to be uninstalled, and then click **Delete** in the Actions column. **Note** Approximately 2 minutes is required to remove the server from the anti-ransomware policy. Wait until the server is removed. 2. Apply the anti-ransomware policy to the server. For more information, see Edit an anti-ransomware policy. 3. Reinstall the anti-ransomware agent.
INSTALL_FAILED	Installation failed	The anti-ransomware agent fails to be installed because the execution of the Cloud Assistant command times out.	Perform the following operations to reinstall the anti-ransomware agent: 1. Log on to the . On the Anti-blackmail page, click the **Server extortion virus protection** tab. On the Server extortion virus protection tab, uninstall the anti-ransomware agent. After you uninstall the anti-ransomware agent, the status of the agent changes to **Not Installed**. 2. Reinstall the anti-ransomware agent.
			Perform the following operations to clear the registry entries and reinstall the agent: 1. Log on to the . On the Anti-blackmail page, click the **Server extortion virus protection** tab. On the Server extortion virus protection tab, uninstall the anti-ransomware agent. After you uninstall the anti-ransomware agent, the status of the agent changes to **Not Installed**. 2. Clear the following registry entries based on the version of the anti-ransomware agent that is installed based on anti-ransomware policies: ○ The registry entries of the V1.X.X anti-ransomware agent

Error code	Information in the Details message	Cause	Solution

AGENT_NOT_RUN_AFTER_INSTALLATION	Post-installation services not started	After you install the anti-ransomware agent, the agent is not started because some registry entries of the agent that you previously uninstall are retained.	`# The V1.X.X anti-ransomware agent`
			`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\hybridbackup`
			`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\hbrupdater`
			○ The registry entries of the V2.X.X anti-ransomware agent
			`# The V2.X.X anti-ransomware agent`
			`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\hbrclient`
			`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\hbrclientupdater`
			`HKEY_LOCAL_MACHINE\SOFTWARE\Alibaba, Inc.\Aliyun Hybrid Backup Service Client`
			`# 64-bit`
			`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B1F066FC-D85C-46F8-9ED7-88A4385AF9A6}}_is1`
			`# 32-bit`
			`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9A3FBAB2-A9B0-4F3B-951A-ABC72D58BA6D}}_is1`
			3. Reinstall the anti-ransomware agent.

FAILED_TO_DOWNLOAD_INSTALLER	Failed to download the installation package	The installation package of the anti-ransomware agent fails to be downloaded because the network connection fails.	Perform the following operations to troubleshoot network connection issues: 1. Log on to your ECS instance, run the `ping` or `telnet` command to test the connectivity between the ECS instance and the anti-ransomware endpoint, and then check whether firewall policies are configured for the ECS instance. For more information about anti-ransomware endpoints, see Anti-ransomware endpoints. 2. After you troubleshoot network connection issues, reinstall the anti-ransomware agent.

Error code	Information in the Details message	Cause	Solution
PRECHECK_COMMAND_FAILED	Preflight command failed	The execution of the Cloud Assistant command times out.	Perform the following operations to reinstall the anti-ransomware agent: 1. Log on to the . On the Anti-blackmail page, click the **Server extortion virus protection** tab. On the Server extortion virus protection tab, uninstall the anti-ransomware agent. After you uninstall the anti-ransomware agent, the status of the agent changes to **Not Installed**. 2. Reinstall the anti-ransomware agent.
INSTALL_COMMAND_TIMEOUT	Install Command timeout	The anti-ransomware agent fails to be installed because the installation command times out.	Perform the following operations to reinstall the anti-ransomware agent: 1. Log on to the . On the Anti-blackmail page, click the **Server extortion virus protection** tab. On the Server extortion virus protection tab, uninstall the anti-ransomware agent. After you uninstall the anti-ransomware agent, the status of the agent changes to **Not Installed**. 2. Reinstall the anti-ransomware agent.
ServiceUnavailable	ServiceUnavailable	Your Alibaba Cloud account does not have the required permissions, or the QPS exceeds the upper limit.	- Log on to the Security Center console by using your Alibaba Cloud account. On the Anti-blackmail page, click the **Server extortion virus protection** tab. On the Server extortion virus protection tab, click **Authorize Now** to assign the **AliyunHBRDefaultRole** and **AliyunECSAccessingHBRRole** roles to your Alibaba Cloud account. - If you want to increase the QPS limit, .
CONFLICT_WITH_EXISTING_AGENT	Conflict with existing client	The anti-ransomware agent fails to be installed because the agent is installed.	Perform the following operations to reinstall the anti-ransomware agent: 1. Log on to the . On the Anti-blackmail page, click the **Server extortion virus protection** tab. On the Server extortion virus protection tab, uninstall the anti-ransomware agent. After you uninstall the anti-ransomware agent, the status of the agent changes to **Not Installed**. 2. Reinstall the anti-ransomware agent.

Error code	Information in the Details message	Cause	Solution
ACTIVATE_COMMAND_FAILED	An error occurs on the client. You need to reinstall the client to restore normal service operation. If the failure persists, submit a ticket for consultation. Alibaba technical experts will help you troubleshoot the issue.	An error occurs on the anti-ransomware agent.	Perform the following operations to reinstall the anti-ransomware agent: 1. Log on to the . On the Anti-blackmail page, click the **Server extortion virus protection** tab. On the Server extortion virus protection tab, uninstall the anti-ransomware agent. After you uninstall the anti-ransomware agent, the status of the agent changes to **Not Installed**. 2. Reinstall the anti-ransomware agent. 3. If the anti-ransomware agent fails to be installed, to address the issue.
CHECK_RUNNING_COMMAND_FAILED	Check service startup command failed	A service error occurs.	Perform the following operations to reinstall the anti-ransomware agent: 1. Log on to the . On the Anti-blackmail page, click the **Server extortion virus protection** tab. On the Server extortion virus protection tab, uninstall the anti-ransomware agent. After you uninstall the anti-ransomware agent, the status of the agent changes to **Not Installed**. 2. Reinstall the anti-ransomware agent.

The following table describes the anti-ransomware endpoints in different regions.

Region	Public endpoint	ECS internal endpoint
China (Hangzhou)	https://hbr.cn-hangzhou.aliyuncs.com	https://hbr-vpc.cn-hangzhou.aliyuncs.com
China (Shanghai)	https://hbr.cn-shanghai.aliyuncs.com	https://hbr-vpc.cn-shanghai.aliyuncs.com
China (Qingdao)	https://hbr.cn-qingdao.aliyuncs.com	https://hbr-vpc.cn-qingdao.aliyuncs.com
China (Beijing)	https://hbr.cn-beijing.aliyuncs.com	https://hbr-vpc.cn-beijing.aliyuncs.com
China (Zhangjiakou)	https://hbr.cn-zhangjiakou.aliyuncs.com	https://hbr-vpc.cn-zhangjiakou.aliyuncs.com

Region	Public endpoint	ECS internal endpoint
China (Hohhot)	https://hbr.cn-huhehaote.aliyuncs.com	https://hbr-vpc.cn-huhehaote.aliyuncs.com
China (Shenzhen)	https://hbr.cn-shenzhen.aliyuncs.com	https://hbr-vpc.cn-shenzhen.aliyuncs.com
China (Chengdu)	https://hbr.cn-chengdu.aliyuncs.com	https://hbr-vpc.cn-chengdu.aliyuncs.com
China (Hong Kong)	https://hbr.cn-hongkong.aliyuncs.com	https://hbr-vpc.cn-hongkong.aliyuncs.com
Singapore (Singapore)	https://hbr.ap-southeast-1.aliyuncs.com	https://hbr-internal.ap-southeast-1.aliyuncs.com
Australia (Sydney)	https://hbr.ap-southeast-2.aliyuncs.com	https://hbr-vpc.ap-southeast-2.aliyuncs.com
Malaysia (Kuala Lumpur)	https://hbr.ap-southeast-3.aliyuncs.com	https://hbr.ap-southeast-3.aliyuncs.com
Indonesia (Jakarta)	https://hbr.ap-southeast-5.aliyuncs.com	https://hbr-vpc.ap-southeast-5.aliyuncs.com
Japan (Tokyo)	https://hbr.ap-northeast-1.aliyuncs.com	https://hbr.ap-northeast-1.aliyuncs.com
Germany (Frankfurt)	https://hbr.eu-central-1.aliyuncs.com	https://hbr.eu-central-1.aliyuncs.com
US (Silicon Valley)	https://hbr.us-west-1.aliyuncs.com	https://hbr.us-west-1.aliyuncs.com

Alibaba Finance Cloud

Region	Public endpoint	ECS internal endpoint
China East 2 Finance	https://hbr.cn-shanghai-finance-1.aliyuncs.com	https://hbr-vpc.cn-shanghai-finance-1.aliyuncs.com

1.3.4. Release disk space occupied by backup caches

To improve the efficiency of data backup, the anti-ransomware feature caches data during the backup. By default, data backup caches occupy disk space on your server. If the backup cache files that are stored in a directory on your server occupy a large volume of disk space, you can release the disk space of the directory. To release the disk space, clear the backup cache files in the directory or store the backup cache files in a different directory.

Context

In most cases, backup files are temporarily stored on a disk of your server and backup caches are generated. After the backup files are uploaded to the cloud, the backup caches are automatically deleted from the disk. If a large number of backup files exist, the size of a backup file is large, or a program does not run as expected, the backup caches may occupy a large volume of disk space. We recommend that you clear backup caches on a regular basis to improve server performance.

Clear backup caches

To clear backup caches, perform the following steps:

1. If the client protection feature is enabled for your server, disable the feature for your server.

   If the client protection feature is enabled for your server, Security Center automatically protects the files that are stored in the directory of the Security Center agent. If you want to modify the files in the directory of the Security Center agent and clear cache files, you must disable client protection for the server. For more information about the client protection feature, see Use the client protection feature.

2. Log on to the server as the root user.

3. Clear the backup cache files that are stored in the directory on your server.

   The following table lists the directory in which the backup cache files are stored for each version of the anti-ransomware agent.

Client version	Operating system of the server	Directory in which the backup cache files are stored
1.X.X	Windows	*C:\Program Files (x86)\Alibaba\Aegis\hbr\cache*
	Linux	*/usr/local/aegis/hbr/cache*
2.X.X	Windows	*C:\Program Files (x86)\Alibaba\Aegis\hbrclient\cache*
	Linux	*/usr/local/aegis/hbrclient/cache*

> **Note** After you enable the anti-ransomware feature for your server, the feature backs up the files that are specified in the protection policy. If you delete the cache files, the backup files are not affected.

Modify backup cache configurations

1. Log on to the server as the root user.

2. Go to the directory in which the anti-ransomware agent is installed.

   The following table lists the installation directory of each version of the anti-ransomware agent.

Client version	Operating system of the server	Installation directory of the anti-ransomware agent
1.X.X	Windows	*C:\Program Files (x86)\Alibaba\Aegis\hbr\client*
	Linux	*/usr/local/aegis/hbr/client*
	Windows	*C:\Program Files (x86)\Alibaba\Aegis\hbrclient\client*

2.X.X Client version	Operating system of the server	Installation directory of the anti-ransomware agent
	Linux	*/usr/local/aegis/hbrclient/client*

3. Create a file named `hbr.config` in the `client` folder.
4. In the `hbr.config` file, configure the parameters that are described in the following table to add data IDs and metadata caches. Then, save the file.

   You can configure the parameters in the `hbr.config` file to specify the directory in which the caches are stored and the upper limit of the system memory that the caches can occupy.

Parameter	Description
disable_blob_cache	Specifies whether to cache data entry IDs. Valid values: ○ **true**: does not cache data entry IDs. ○ **false**: caches data entry IDs.
max_blob_cache_weight	The maximum percentage of system memory that cached data entry IDs can occupy. The value must between 0 and 1. The default value is 0.15, which indicates that the cached data entry IDs can occupy up to 15% of system memory.
cache_prefix	The path in which the caches are stored. The path must be an absolute path.
max_retain_count	The maximum number of cached data entry IDs that can be retained. The value must be an integer.
disable_file_cache	Specifies whether to cache metadata. Valid values: ○ **true**: does not cache metadata. ○ **false**: caches metadata.
file_cache_max_size_hint	The maximum disk space that the metadata cache files can occupy. The actual disk space occupied by the files may exceed the specified value. Default value: 2 GB. **Note** ○ If you set the parameter to 2 GB, you can back up a minimum of 4 TB of metadata. ○ The value of the parameter cannot exceed the available disk space. ○ If you specify a value that is too small, the backup does not fail but the cache performance is decreased.

The following example shows the configurations of the hbr.config file:

```
disable_blob_cache = false    // Cache data entry IDs.
max_blob_cache_weight = 0.15    // Cached data entry IDs can occupy up to 15% of system
memory.
cache_prefix = D:\CacheFolder    // The caches are stored in D:\CacheFolder.
max_retain_count = 16    // Up to 16 cached data entry IDs can be retained.
disable_file_cache = false    // Cache metadata.
file_cache_max_size_hint = 2g    // Cached metadata can occupy up to 2 GB of disk space
.
```

Note After you change the directory in which the cache files are stored, you do not need to restart the anti-ransomware agent. The new configuration automatically takes effect upon the next backup.

1.4. Enable anti-ransomware for databases

1.4.1. Create an anti-ransomware policy

Security Center provides the feature of anti-ransomware for databases. You can use the feature to create an anti-ransomware policy to back up data in your database. If your database is intruded by ransomware, you can restore the data of your database by using backups. This ensures that your workload runs as expected. This topic describes how to create an anti-ransomware policy for a database.

Context

If you use Alibaba Cloud Hybrid Backup Recovery (HBR) to back up the data in your database, we recommend that you do not use the feature of anti-ransomware for databases to back up the data in your database.

Prerequisites

A specific amount of anti-ransomware capacity is purchased. The permissions to use anti-ransomware are granted. For more information, see Enable anti-ransomware.

Procedure

1.
2. In the left-side navigation pane, choose **Defense > Anti-ransomware**.
3. On the **Anti-blackmail** page, click the **Database extortion virus protection** tab and click **Create Policies**.
4. In the **Database protection strategy** panel, create an anti-ransomware policy for a database.

i. In the Change database step, configure the following parameters and click **Next**.

Parameter	Description
Policy Name	The name of the anti-ransomware policy.
Type	The method that you want to use to select the database. Valid values: - **Automatic identification database** The system automatically identifies the databases that are deployed on your server. We recommend that you select this option. - **Manually enter the database** If the database that you want to protect is not displayed in the list of databases after you select **Automatic identification database**, you can select this option and manually specify the database.
Database	The database that you want to protect or the server in which the database resides.
Database type	The type of the database that you want to protect. This parameter is required only if you set the Type parameter to **Manually enter the database**. Valid values: - MYSQL - ORACLE - MSSQL
Account	The username of the account that you can use to log on to the required database. The account must have the permissions to back up data in the database. If you set the Database type parameter to ORACLE, you do not need to enter the username or the password of the database. **Notice** You must enter the username and password of the database instead of the server.
Password	The password of the account that you can use to log on to the database.

ii. In the Protection Policies step, configure the following parameters and click **Finished**.

Parameter	Description
Protection Policies	The anti-ransomware policy that you want to use. You can click **Use recommendation strategy** to use the recommended anti-ransomware policy that is provided by Security Center. If the recommended anti-ransomware policy cannot meet your business requirements, you can modify the policy.
Full backup strategy	The interval at which full backup is performed, the days of a week on which full backup is performed, and the point in time at which the full backup starts. Full backup indicates that you back up all data that exists at a specific point in time. Full backup is time-consuming and requires a large amount of anti-ransomware capacity.
Incremental backup strategy	The interval at which incremental backup is performed and the point in time at which the incremental backup starts. Incremental backup indicates that you back up only the data that is newly generated or modified after the last full or incremental backup. Therefore, incremental backup is time-saving and requires less anti-ransomware capacity.
Backup data retention time	The retention period of the backup.
Backup network bandwidth limit	The maximum network bandwidth that is allowed during data backup. If you set this parameter to 0, network bandwidth is unlimited.

After the anti-ransomware policy for your database is created, Security Center automatically installs the anti-ransomware agent on your server, and the policy enters the **Initializing** state. After the anti-ransomware agent is installed on your server, Security Center backs up data in your database based on the backup policy that is configured in the anti-ransomware policy.

What to do next

After the anti-ransomware policy is created, you must precheck the database that is specified in the policy. If the precheck is successful, you can back up the data in the database. For more information, see Precheck a database.

After the anti-ransomware policy for your database is created, we recommend that you monitor the status of the anti-ransomware policy. If the policy is abnormal, perform troubleshooting at the earliest opportunity. For more information, see Troubleshoot the issues causing the abnormal status of an anti-ransomware policy for a database.

1.4.2. Precheck a database

After you create an anti-ransomware policy for a database, you must precheck the connectivity between not only the database and Object Storage Service (OSS) but also the database and the control network. If the precheck succeeds, you can back up the data in the database. Anti-ransomware for databases is available only for MySQL databases, Oracle databases, and SQL Server databases that are deployed on Elastic Compute Service (ECS) instances. This topic describes how to precheck database instances.

Context

Context

If you want to back up data in MySQL databases, Oracle databases, or SQL Server databases that are deployed on ECS instances, you need to pay attention to the database versions and backup features that are supported by each version. For more information, see Overview.

Procedure

1.
2. In the left-side navigation pane, choose **Defense > Anti-ransomware**.
3. On the **General Anti-ransomware Solutions** page, click the **Database extortion virus protection** tab.
4. In the anti-ransomware policy list, find the newly created policy and click **Pre-check** in the **Actions** column.
5. In the Pre-check dialog box, click **Starting**.
    - Check items for a MySQL database

Check item	Description
OSS connectivity	Checks whether the MySQL database is connected to the VPC Access from ECS (Internal Network) endpoint of an OSS bucket. The instance and the bucket must reside in the same region. If the connectivity check fails, you cannot back up or restore data in the database.
Control network connectivity	Checks whether the MySQL database is connected to the control network. If the connectivity check fails, you cannot back up or restore data in the database.
Versions of databases that support full backup	Checks whether the version of the MySQL database supports full backup. **Note** MySQL 8.0 does not support incremental backup.
Binary log check	Checks whether the binary log configuration of the MySQL database is valid. If the check fails, you cannot back up or restore data in the database.

    - Check items for an Oracle database

Check item	Description
OSS connectivity	Checks whether the Oracle database instance is connected to the VPC Access from ECS (Internal Network) endpoint of an OSS bucket. The instance and the bucket must reside in the same region. If the connectivity check fails, you cannot back up or restore data in the database.
Control network connectivity	Checks whether the Oracle database instance is connected to the control network. If the connectivity check fails, you cannot back up or restore data in the database.

Check item	Description
Status of the Oracle database instance	Checks whether the Oracle database instance runs as expected. If the instance does not run as expected, you cannot back up or restore data in the database.
Oracle database status	Checks whether all Oracle databases in the Oracle database instance run as expected. If a database in the instance does not run as expected, you cannot back up or restore data in the database.
Archive mode	Checks whether the archive mode can be enabled for the Oracle database instance. If the check fails, you cannot back up or restore data in the database. For more information about how to enable the archive mode, see Enable archive mode for an Oracle database.

- Check items for a SQL Server database

Check item	Description
OSS connectivity	Checks whether the SQL Server database is connected to the VPC Access from ECS (Internal Network) endpoint of an OSS bucket. The database and the bucket must reside in the same region. If the connectivity check fails, you cannot back up or restore data in the database.
Control network connectivity	Checks whether the SQL Server database is connected to the control network. If the connectivity check fails, you cannot back up or restore data in the database.
Recovery model	Checks the recovery model of the SQL database. If the check fails, you cannot perform incremental backups or log backups in the database. Notice ■ Due to the limits of SQL Server, databases that fail the check support only the SIMPLE recovery model. You cannot perform log backups on these databases. ■ You can perform only full backups on master databases. If you perform an incremental backup or log backup for a master database, the system automatically implements full backup instead. ■ For more information about how to change the recovery model, see SQL Server documentation.

Check item	Description
SQL Server database status	Checks whether the SQL Server database runs as expected. If the database does not run as expected, you cannot back up or restore data in the database.

The precheck takes about 1 minute.
If an item fails the precheck, follow the on-screen instructions to check whether the failure affects the backup and restoration operations in the database. If the failure affects the backup and restoration operations, we recommend that you handle the issue at the earliest opportunity based on this topic.

1.4.3. Manage an anti-ransomware policy

After you create an anti-ransomware policy, you can disable or edit the anti-ransomware policy. If you no longer need the anti-ransomware policy, you can delete it. This topic describes how to disable, edit, and delete an anti-ransomware policy. This topic also describes how to manually install and uninstall the anti-ransomware agent.

Prerequisites

An anti-ransomware policy is created for your database. For more information, see Create an anti-ransomware policy.

Context

If the status of the anti-ransomware policy is **Successful**, the anti-ransomware policy takes effect. In this case, the data in your database is backed up based on the anti-ransomware policy. If the status of the anti-ransomware policy is **Execution failed**, we recommend you handle the exception at the earliest opportunity. For more information, see Troubleshoot the issues causing the abnormal status of an anti-ransomware policy for a database.

Enable or disable an anti-ransomware policy

1.
2. In the left-side navigation pane, choose **Defense > Anti-ransomware**.
3.
4. In the anti-ransomware policy list, find the anti-ransomware policy that you want to enable or disable and turn on or turn off the switch in the **Policy status** column.
   - **Disable an anti-ransomware policy**
     To disable an anti-ransomware policy, find the anti-ransomware policy and turn off the switch in the **Policy status** column.

     > **Notice** After you disable the anti-ransomware policy, the data backup task that runs based on the anti-ransomware policy stops. Proceed with caution.

   - **Enable an anti-ransomware policy**
     The anti-ransomware agent can back up the data in your database based on an anti-ransomware policy only after the anti-ransomware policy is enabled. This protects your database against ransomware. To enable an anti-ransomware policy, turn on the switch in the **Policy status** column.

Edit an anti-ransomware policy

After an anti-ransomware policy is created, you can edit the anti-ransomware policy.

1.
2. In the left-side navigation pane, choose **Defense > Anti-ransomware**.
3.
4. In the anti-ransomware policy list, find the anti-ransomware policy that you want to edit and click **Edit** in the **Actions** column.
5. In the **Database protection strategy** panel, change the value of **Policy Name**.
6. Enter the username and password of your database account and click **Next**.
7. Configure the parameters.

Parameter	Description
Protection Policies	The anti-ransomware policy that you want to use. You can click **Use recommendation strategy** to use the recommended anti-ransomware policy that is provided by Security Center. If the recommended anti-ransomware policy cannot meet your business requirements, you can modify the policy.
Full backup strategy	The interval at which full backup is performed, the days of a week on which full backup is performed, and the point in time at which the full backup starts. Full backup indicates that you back up all data that exists at a specific point in time. Full backup is time-consuming and requires a large amount of anti-ransomware capacity.
Incremental backup strategy	The interval at which incremental backup is performed and the point in time at which the incremental backup starts. Incremental backup indicates that you back up only the data that is newly generated or modified after the last full or incremental backup. Therefore, incremental backup is time-saving and requires less anti-ransomware capacity.
Backup data retention time	The retention period of the backup.
Backup network bandwidth limit	The maximum network bandwidth that is allowed during data backup. If you set this parameter to 0, network bandwidth is unlimited.

8. Click **Finished**.

   The anti-ransomware agent backs up the data in your database based on the new anti-ransomware policy.

Delete an anti-ransomware policy

If you no longer need an anti-ransomware policy, you can delete it.

1.
2. In the left-side navigation pane, choose **Defense > Anti-ransomware**.
3.

4. In the anti-ransomware policy list, find the anti-ransomware policy that you want to delete and click the ⋮ icon in the **Actions** column.
5. Select **Delete** from the drop-down list.
6. In the message that appears, click **OK**.

   Wait until the anti-ransomware policy is deleted.

Manually install the anti-ransomware agent

If an anti-ransomware policy for a database fails to be initialized or you have manually uninstalled the anti-ransomware agent from the server on which the anti-ransomware policy takes effect, you can manually install the anti-ransomware agent on the server.

1.
2. In the left-side navigation pane, choose **Defense > Anti-ransomware**.
3.
4. In the anti-ransomware policy list, find the anti-ransomware policy for which you want to install the anti-ransomware agent, and click the ⋮ icon in the **Actions** column.
5. Select **Install the client** from the drop-down list.
   The value of **Client status** for the anti-ransomware policy changes to **Installing**. The anti-ransomware agent is installed in about 5 minutes.

Manually uninstall the anti-ransomware agent

> **Notice** After you uninstall the anti-ransomware agent, the anti-ransomware policy that is created for your database no longer backs up the data of your database, and your database is not protected from ransomware. Proceed with caution.

1.
2. In the left-side navigation pane, choose **Defense > Anti-ransomware**.
3.
4. In the anti-ransomware policy list, find the anti-ransomware policy for which you want to uninstall the anti-ransomware agent and click the ⋮ icon in the **Actions** column.
5. Select **Uninstall Client** from the drop-down list.
6. In the message that appears, click **OK**.
   The value of **Client status** for the anti-ransomware policy changes to **Uninstalling**. The anti-ransomware agent is uninstalled in about 5 minutes.

1.4.4. Create a restoration task

If the data in your database is encrypted by ransomware, you can create a restoration task to restore the encrypted data and reduce loss. This topic describes how to create a restoration task and view the status of the restoration task.

Prerequisites

- An anti-ransomware policy is created for your database and is enabled. Data can be backed up based on the policy.

- The number of backup versions is not zero.

Procedure

1.
2. In the left-side navigation pane, choose **Defense > Anti-ransomware**.
3.
4. In the anti-ransomware policy list, find the database whose data you want to restore and click **Recovery** in the **Actions** column.
5. In the **Restoration** dialog box, configure the parameters.

   The parameters vary based on database engines.

   > **Notice** If you have a server that runs the same operating system as the original server hosting the database and a protection server is protected for the server, you can restore your data to the server. However, you cannot restore the data to a server that runs a different operating system from the original server.

   - Parameters required to restore the data in MySQL databases

Parameter	Description
Recovery time point	The time at which the selected backup is generated. If the data in your database is encrypted by ransomware, you can select the last backup version before the encryption. This way, the restored data is similar to the data before the encryption.
Restore to server	The server to which you want to restore your data.

   - Parameters required to restore the data in SQL Server databases

Parameter	Description
Change database	The database whose data you want to restore.
List of stored backups	The backup that you want to use to restore data. If the data in your database is encrypted by ransomware, you can select the last backup version before the encryption. This way, the restored data is similar to the data before the encryption.
Restore to server	The server to which you want to restore your data.

   - Parameters required to restore the data in Oracle databases

Parameter	Description
Select recovery version	The version of the backup that you want to use to restore data. The value of this parameter is a time range in which the data is backed up.
Recovery time point	The time at which the selected backup is generated. You can set this parameter to any time within the time range in which the data is backed up.
Restore to server	The server to which you want to restore your data.

6. Click **OK**.

   The anti-ransomware agent runs the restoration task.

   > Notice If a data backup task and a restoration task are running on the server that you specify at the same time, the restoration task fails. We recommend that you stop the data backup task that is running on the server before you create a restoration task.

View a restoration task

You can view a restoration task in the **Recovery record** panel. To go to the panel, click the value below **Recovering/Recovering Records** on the Database extortion virus protection tab. After the restoration task is complete, the value in the **Recovery Status** column changes to **Successful** in the **Recovery record** panel.

1.4.5. Troubleshoot the issues causing the abnormal status of an anti-ransomware policy for a database

If you create an anti-ransomware policy for your database and the status of the anti-ransomware policy is abnormal in the Security Center console, you can troubleshoot the issues causing the abnormal status by following the instructions that are provided in this topic. The abnormal status includes Wrong account password, Initializing, initialization failed and Excess is automatically closed.

Prerequisites

An anti-ransomware policy is created for your database. For more information, see Create an anti-ransomware policy.

Context

If the status of the anti-ransomware policy is abnormal, the system cannot back up the data in your database. Your database cannot be protected against anti-ransomware attacks. We recommend that you troubleshoot the issues causing the abnormal status of the anti-ransomware policy at the earliest opportunity.

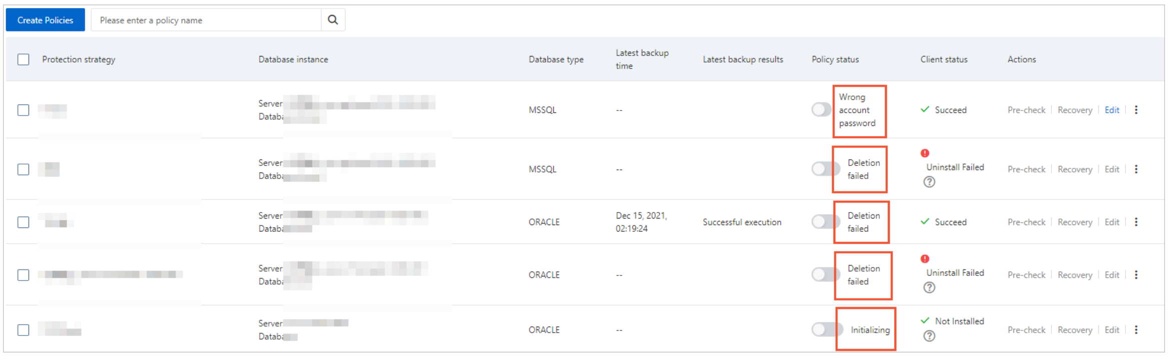
Procedure

1.

2.

3.

4. On the **Database extortion virus protection** tab, view the causes of the abnormal status of the anti-ransomware policy.



Create Policies | Please enter a policy name

□	Protection strategy	Database instance	Database type	Latest backup time	Latest backup results	Policy status	Client status	Actions
□	[redacted]	Server [redacted] Datab [redacted]	MSSQL	--		Wrong account password	✓ Succeed	Pre-check | Recovery | Edit | ⋮
□	[redacted]	Server [redacted] Datab [redacted]	MSSQL	--		Deletion failed	Uninstall Failed	Pre-check | Recovery | Edit | ⋮
□	[redacted]	Server [redacted] Datab [redacted]	ORACLE	Dec 15, 2021, 02:19:24	Successful execution	Deletion failed	✓ Succeed	Pre-check | Recovery | Edit | ⋮
□	[redacted]	Server [redacted] Datab [redacted]	ORACLE	--		Deletion failed	Uninstall Failed	Pre-check | Recovery | Edit | ⋮
□	[redacted]	Server [redacted] Datab [redacted]	ORACLE	--		Initializing	✓ Not Installed	Pre-check | Recovery | Edit | ⋮

5. Troubleshoot the issues based on the causes.

   For more information about the causes and solutions, see the "Policy states" section of this topic.

Policy states

State	Description	Solution
Wrong account password	The username or password of your database is invalid.	Enter the correct username and password of your database. Then, enable the anti-ransomware policy again.
Initializing	The anti-ransomware policy is being initialized.	Wait until the anti-ransomware policy is initialized.
initialization failed	The anti-ransomware policy failed to be initialized.	Reinstall the anti-ransomware agent. Then, edit the anti-ransomware policy. For more information about how to install the anti-ransomware agent, see Manually install the anti-ransomware agent. For more information about how to edit an anti-ransomware policy, see Edit an anti-ransomware policy.
Enabling	The anti-ransomware policy is being enabled.	Wait until the anti-ransomware policy is enabled.
Enabled	The anti-ransomware policy is enabled.	None.
Discontinued	The anti-ransomware policy is disabled.	None.
Disabling	The anti-ransomware policy is being disabled.	Wait until the anti-ransomware policy is disabled.

State	Description	Solution
Excess is automatically closed	The anti-ransomware capacity is insufficient.	Manually delete historical data to release capacity or purchase additional anti-ransomware capacity. For more information, see What do I do if the anti-ransomware capacity that I purchased is insufficient?
Deleting	The anti-ransomware policy is being deleted.	Wait until the anti-ransomware policy is deleted.
Deletion failed	The anti-ransomware policy failed to be deleted.	Try again later. For more information about how to delete an anti-ransomware policy, see Delete an anti-ransomware policy.
Recovering	The data in your database is being restored.	Wait until the data in your database is restored.
Backup in progress	The data in your database is being backed up.	Wait until the data in your database is backed up.

2.Overview

Persistent viruses, such as ransomware and mining programs, have become major threats to network security. To prevent persistent viruses from intruding into your servers, Security Center provides the antivirus feature to scan for persistent viruses and generates alerts when persistent viruses are detected. This feature also supports virus deep cleaning and data backup.

Background information

Before you use the antivirus feature, we recommend that you turn on **Virus Blocking** on the **Settings** page. After you turn on **Virus Blocking**, Security Center automatically detects and removes common trojans, ransomware, mining viruses, and DDoS trojans. For more information, see Use proactive defense.

> **Note** The antivirus feature supports a limited number of operating system versions. Servers that use unsupported operating system versions cannot use the data backup feature. For more information about supported operating system versions, see Supported operating system versions.

Features

The antivirus feature provides a general anti-ransomware solution. For more information, see How it works. The antivirus feature also provides the following capabilities:

- **Virus scan**
  The security experts of Security Center conduct automatic analysis on attack methods based on a large number of persistent virus samples. Alibaba Cloud develops a machine learning antivirus engine based on the attack analysis results. Virus scan uses the machine learning antivirus engine and a virus library that is updated in real time. Virus scan allows you to detect viruses at the earliest opportunities. You can create virus scan tasks to check whether your servers are intruded by viruses. For more information, see Scan for viruses.
- **Alert management**
  The antivirus feature allows you to manage virus alerts. You can perform deep cleaning tasks on persistent viruses, such as ransomware and mining programs. Virus deep cleaning can remove persistent viruses by terminating virus processes, quarantining malicious files, and removing inserted viruses. For more information, see Handle virus alerts.
- **Data backup**
  The antivirus feature provides the capability of anti-ransomware data backup. If your servers are intruded by ransomware, you can use data backup to restore data and reduce loss. You can create protection policies to back up the data of core servers. For more information, see Create an anti-ransomware policy. If you want to restore server data, you can create restoration tasks. For more information, see Create a restoration task.

How it works

Ransomware has been a major threat to enterprises and individuals. If the core data or files stored on the servers are encrypted by attackers, paying the ransom is the only solution. Ransomware has caused tremendous loss to numerous enterprises and individuals. To help enterprises and individuals handle ransomware, Alibaba Cloud releases a general anti-ransomware solution. This solution provides layer-by-layer protection against ransomware.

The **general anti-ransomware solution** provides a layer-by-layer protection system against ransomware.

- **Block recognized ransomware in real time**

Security Center has blocked a large amount of ransomware recognized by the Alibaba Cloud intelligence library. Security Center blocks ransomware at the earliest opportunity to prevent potential loss.

- **Trap and block new ransomware**
  Security Center sets trap directories to block potential ransomware activities. To block new ransomware, Security Center immediately blocks unusual encryption activities when they are detected. In addition, Security Center generates alerts to notify you of the potential threats.

  > **Note** On the **Settings** page of the , turn on **Anti-ransomware (Bait Capture)** in the **Proactive Defense** section of the General tab. For more information, see Use proactive defense. After you turn on Anti-ransomware (Bait Capture), Security Center sets trap directories on your servers to block potential ransomware activities. If you find a suspicious directory on your server, contact after-sales services or submit a ticket to check whether the directory is a trap directory set by Security Center. Trap directories do not affect your workloads and are not malicious. Trap directories cannot be manually deleted.

- **Restore infected files**
  In addition to anti-ransomware, Security Center supports data backup. This feature periodically backs up data and allows you to restore server data based on the specified time or file version. In scenarios in which files on your servers are encrypted, you can restore the data to ensure the security of your servers.

Supported operating system versions

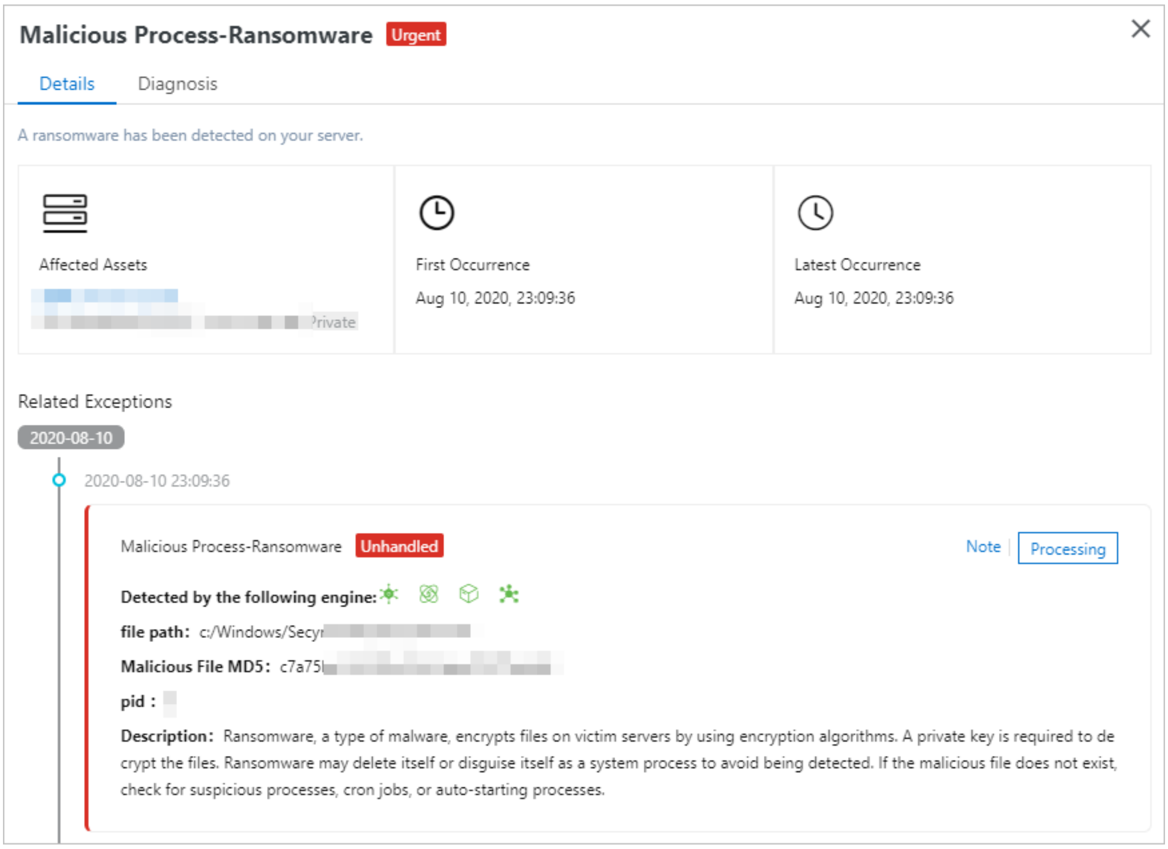
Operating system	Supported version
Windows	7, 8, and 10
Windows Server	2008 R2, 2012, 2012 R2, 2016, and 2019
Red Hat Enterprise Linux (RHEL)	7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 7.8, 8, 8.1, and 8.2
CentOS	6.5, 6.9, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.2, and 8.3
Ubuntu	14.04, 16.04, 18.40, and 20.04
SUSE Linux Enterprise Server	11, 12, and 15

Antivirus suggestions

When you use Security Center to block ransomware, perform the following steps:

1. **Before the process: Enable the antivirus feature and create protection polices**
   The antivirus feature provides the data backup capability. You must enable the antivirus feature and create protection polices to back up the core data of your servers. For more information, see Enable anti-ransomware and Create an anti-ransomware policy.
2. **During the process: Handle ransomware alerts and create restoration tasks**

Security Center generates alerts when ransomware activities are detected. If you receive ransomware alerts, we recommend that you troubleshoot the causes and handle the alerts at the earliest opportunity. For more information, see View and handle alerts. If the data on your servers is encrypted by ransomware, you can create restoration tasks to restore the encrypted data. For more information, see Create a restoration task.



Malicious Process-Ransomware Urgent

Details Diagnosis

A ransomware has been detected on your server.

Affected Assets

[redacted] 'rivate

First Occurrence

Aug 10, 2020, 23:09:36

Latest Occurrence

Aug 10, 2020, 23:09:36

Related Exceptions

2020-08-10

2020-08-10 23:09:36

Malicious Process-Ransomware Unhandled

Note Processing

Detected by the following engine:

file path: c:/Windows/Secyr[redacted]

Malicious File MD5: c7a75[redacted]

pid : [redacted]

Description: Ransomware, a type of malware, encrypts files on victim servers by using encryption algorithms. A private key is required to de crypt the files. Ransomware may delete itself or disguise itself as a system process to avoid being detected. If the malicious file does not exist, check for suspicious processes, cron jobs, or auto-starting processes.

3. **After the process: Scan for server vulnerabilities and reinforce security**
   To further reduce the risk of ransomware attacks, we recommend that you perform the following steps:
   - Regularly fix system vulnerabilities to prevent vulnerabilities from being exploited by attackers. You can use the vulnerability fixing feature provided by Security Center. For more information, see Overview.
   - Enable two-factor authentication for servers that are important. Do not use weak passwords on your servers.
   - Make sure that only necessary ports are accessible over the Internet.

3.Anti-Virus

3.1. Scan for viruses

For servers that are protected by Security Center, the antivirus feature provides deep scanning services against persistent viruses such as ransomware and mining programs. Security Center supports the immediate and periodic virus scanning methods. This topic describes how to scan for viruses by using the two methods.

Prerequisites

You have purchased the Basic Anti-Virus, Advanced, or Enterprise edition of Security Center. For more information, see Purchase Security Center.

Context

The antivirus feature scans for the following types of viruses:

Immediate and periodic virus scanning can be performed in the following scenarios:

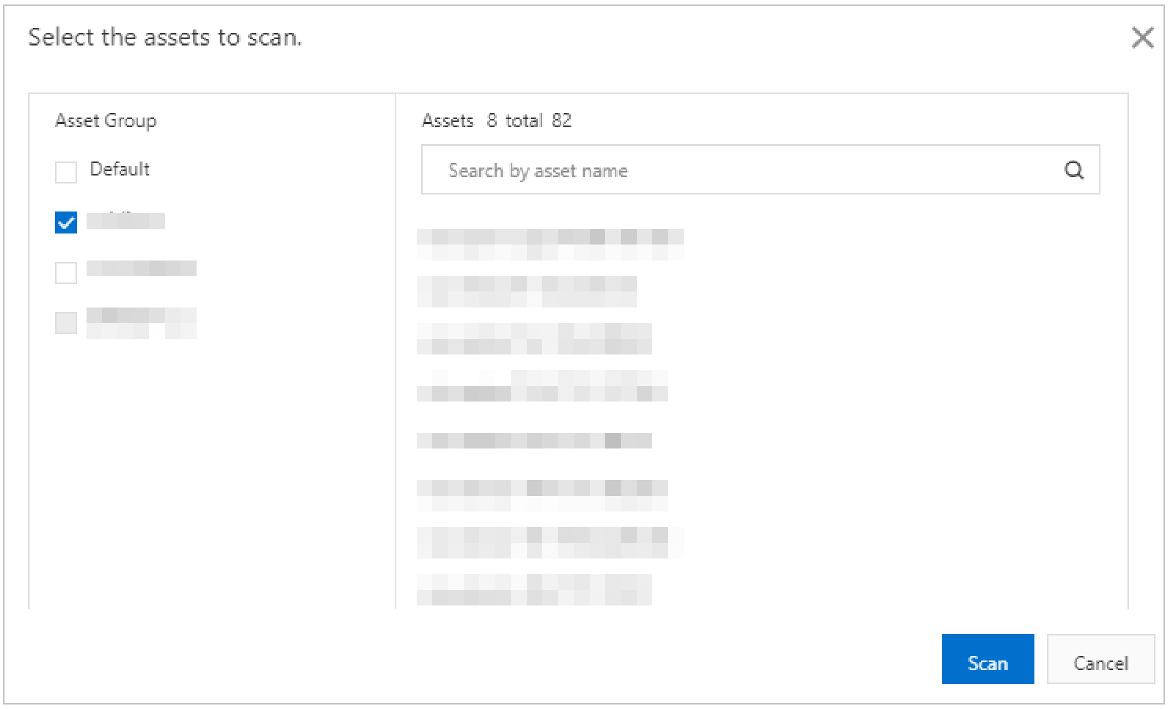
- Immediate virus scanning: All servers in specific asset groups are scanned. You can select all servers from one or more asset groups to scan for viruses.
- Periodic virus scanning: Some or all servers in specific asset groups are scanned.

Immediate virus scanning

To immediately scan for viruses on your server, perform the following steps:

1.
2.
3. On the **Anti-Virus** page, click **Scan Again**.

   If this is your first time to scan for viruses, click **Scan**.
4. In the **Select the assets to scan** dialog box, select one or more **asset groups**.


Select the assets to scan.

Asset Group

□ Default

☑

□

□

Assets 8 total 82

Search by asset name

If you select an asset group in the dialog box, all servers in the asset group are selected by default. You cannot select a specific server from the asset group for scanning. You can select multiple asset groups at a time.

> **Note** You can select only asset groups to scan for viruses. For more information about how to create an asset group, see Create an asset group.

5. Click **Scan**.

   It takes 2 to 5 minutes to complete a scanning task. After the scanning task is complete, we recommend that you check the results and handle the reported alerts at the earliest opportunity. For more information, see Handle virus alerts.

Periodic virus scanning

To periodically scan for viruses on your server, perform the following steps:

1.
2.
3. In the upper-right corner of the **Anti-Virus** page, click **Scan Settings**.
4. In the **Defense Configuration** panel, configure the scan cycle and the assets that you want to scan.

   Configure the scan cycle and the assets that you want to scan based on the following information:

   - **Cycle**: You can set the scan cycle to **3 Days**, **One week**, **Two weeks**, or **Stop**.
   - **Execution Time**: You can set the time range to **00:00-24:00**, **00:00-6:00**, **06:00-12:00**, **12:00-18:00**, or **18:00-24:00**.
   - **Scan Assets**: You can select an asset, an asset group, or multiple assets from asset groups. If you want to periodically scan assets, perform the following operations to select the assets:
     - In the **Asset Group** section, select an asset group. All assets in this asset group are selected. You can remove one or more automatically selected assets from the **Assets** section.
     - In the **Assets** section, enter an asset name and click the 🔍 icon to search for the asset that you want to scan. Fuzzy match is supported.

   > **Note** Based on the scan cycle, Security Center scans for viruses at a random point in time within the time range that you configure.

5. Click **OK**.

> **Notice** If multiple scan cycles are configured, only the scan cycle that you last configure takes effect. Security Center automatically scans for viruses based on the scan cycle that you last configure on your assets.

3.2. Handle virus alerts

Security Center provides the anti-virus feature that supports deep virus scan, virus alerts, and virus alert handling. This topic describes how to use the anti-virus feature to handle virus alerts.

Context

The anti-virus feature provides deep scan and removal of persistent viruses. The anti-virus feature can detect and remove the following virus types:

- Ransomware
- Mining programs
- DDoS Trojans
- Trojans
- Backdoor programs
- Malicious programs
- High-risk programs
- Computer worms
- Suspicious programs
- Automatic mutating Trojans

> **Note** The preceding virus types pose great security threats to your servers. Security Center generates alerts when they are detected. We recommend that you handle virus alerts at the earliest opportunity.

Procedure

1.
2.
3. On the **Anti-Virus** page, click **Process Now**.
4. Find a target alert and click **Processing** in the Actions column.

   To handle multiple alerts simultaneously, select target alerts and click **Batch handled**. To handle all alerts simultaneously, click **Processing**.
5. In the **Alert handling** dialog box that appears, select a method to handle virus alerts.

   The following table lists the methods to handle virus alerts:

Method	Description

Method	Description
Deep cleanup	Select **Deep cleanup** to handle the viruses on you servers. Security Center experts have conducted tests and analysis of persistent viruses. Based on the test and analysis results, deep cleanup is dedicated to handling persistent viruses. Deep cleanup uses the following methods to handle viruses. ○ **Terminate virus processes** Terminates running virus processes to prevent viruses from compromising your service systems. ○ **Quarantine virus files** Quarantines virus files to prevent attackers from starting them. Security Center quarantines virus files. You can download, analyze, and restore quarantined files as needed. For more information, see Use the quarantine feature. ○ **Deleted the persistence method injected by hackers.** Attackers exploit crontab tasks and malicious download sources to implant persistent tasks, which allows attackers to implant more viruses and ensures the persistence of the viruses. Security Center provides dedicated analysis and virus removal to allow you to handle attacks against vulnerable crontab tasks and malicious download sources. In addition, Security Center uses AI learning to enhance the security of your assets and handles viruses within a few hours.
Whitelist	Click **Whitelist** to add an alert to the whitelist. After the alert is added to the whitelist, Security Center no longer generates alerts when the alert event reoccurs.
Ignore	Click **Ignore** to ignore an alert. After you ignore the alert, the status of the alert changes to **Ignored**. If the alert event reoccurs, Security Center will generate alerts.
Handled manually	If you have handled the alert manually, select **Handled manually**. After you select **Handled manually**, the status of the alert changes to **Handled**.

6. Click **Process Now**.

4.Website tamper-proofing

4.1. Overview

Web tamper proofing is a value-added feature provided by Security Center. The feature monitors website directories in real time and can restore tampered files or directories by using backups. The feature also protects important website information from being tampered with and prevents trojans, hidden links, and uploads of violent and illicit content.

Background information

- Web tamper proofing is a value-added feature of Security Center. Security Center does not support the feature. If you use the edition, you must upgrade Security Center to the , , , , or edition before you can purchase and use the feature.
- Web tamper proofing allows you to add processes on Linux and Windows servers to a whitelist. This ensures that protected files are updated in real time.
- To make illegal profits or launch business attacks, attackers exploit vulnerabilities in websites to insert illegal hidden links and tamper with the websites. Defaced web pages affect normal user access and may cause serious economic loss, damaged brand reputation, and political risks.

How web tamper proofing works

The Security Center agent automatically collects the processes that attempt to modify files in the protected directories of the protected servers. The agent identifies suspicious processes and file changes in real time and blocks the suspicious processes that cause file changes.

If you use web tamper proofing, you can set Prevention Mode to one of the following modes:

- **Interception Mode**: Security Center blocks suspicious processes and file changes. This ensures the security of websites and files on your servers. You can view the alerts that are generated for blocked suspicious processes on the **Protection** tab of the Tamper Protection page.
- **Alert Mode**: Security Center identifies suspicious processes and file changes and generates alerts for the identified suspicious processes and file changes. If you cannot determine trusted processes, you can select this mode. You can view alerts and determine whether to add a specific alert to the whitelist on the **Protection** tab of the Tamper Protection page. After you determine trusted processes, we recommend that you set Prevention Mode to Interception Mode for servers that you want to protect. This ensures the security of files on the servers. For more information about how to add alerts to the whitelist, see Add blocked processes to a whitelist.

How the process whitelist ensures normal workloads

You can view the alerts that are generated for unusual file changes, suspicious processes, and the number of times that each suspicious process attempts to modify files on the Tamper Protection page. To go to this page, log on to the Security Center console and choose **Precaution > Tamper Protection**. If a file is modified by a process due to normal workloads, you can add the process to the whitelist. After the process is added to the whitelist, web tamper proofing no longer blocks the process. In scenarios in which the content of websites is frequently modified, the whitelist eliminates the need for you to frequently enable and disable web tamper proofing. The whitelist is suitable for websites such as news and education websites. For more information, see Add blocked processes to a whitelist.

Limits on versions of operating systems and kernels

Web tamper proofing requires that your servers run specific versions of operating systems and kernels. If the versions of operating systems and kernels of your servers are not supported, you cannot add processes to the whitelist and enable the alerting mode of web tamper proofing.

OS version	Kernel version
• CentOS 6.3 • CentOS 6.5 • CentOS 6.6 • CentOS 6.7 • CentOS 6.8 • CentOS 6.9 • CentOS 6.10 • CentOS 7.0-1406 • CentOS 7.1-1503 • CentOS 7.2-1511 • CentOS 7.3-1611 • CentOS 7.4-1708 • CentOS 7.5-1804 • CentOS 7.6-1810 • CentOS 7.7-1908 • CentOS 7.8-2003 • CentOS 7.9-2009	• 2.6.32-**, which indicates all the CentOS kernels whose version numbers start with 2.6.32 • 3.10.0-**, which indicates all the CentOS kernels whose version numbers start with 3.10.0
• CentOS 8.0-1905 • CentOS 8.1-1911 • CentOS 8.2-2004 • CentOS 8.3-2011	• 4.18.0-80.11.2.el8_0.x86_64 • 4.18.0-147.5.1.el8_1.x86_64 • 4.18.0-147.8.1.el8_1.x86_64 • 4.18.0-193.el8.x86_64 • 4.18.0-193.6.3.el8_2.x86_64 • 4.18.0-193.28.1.el8_2.x86_64 • 4.18.0-240.1.1.el8_3.x86_64 • 4.18.0-240.15.1.el8_3.x86_64
Ubuntu 14.04	• 3.13.0-32-generic • 3.13.0-65-generic • 3.13.0-86-generic • 3.13.0-145-generic • 3.13.0-164-generic • 3.13.0-170-generic • 3.19.0-80-generic • 4.4.0-93-generic

OS version	Kernel version
Ubuntu 16.04	4.4.0-62-generic 4.4.0-63-generic 4.4.0-93-generic 4.4.0-117-generic 4.4.0-142-generic 4.4.0-151-generic 4.4.0-154-generic 4.4.0-157-generic 4.4.0-174-generic 4.4.0-178-generic 4.4.0-179-generic 4.4.0-184-generic 4.4.0-194-generic
Ubuntu 18.04	4.15.0-23-generic 4.15.0-42-generic 4.15.0-45-generic 4.15.0-52-generic 4.15.0-70-generic 4.15.0-88-generic 4.15.0-91-generic 4.15.0-109-generic 4.15.0-112-generic 4.15.0-121-generic 4.15.0-124-generic
AliyunOS 2.1903	4.19.81-17.al7.x86_64 4.19.81-17.2.al7.x86_64 4.19.91-18.al7.x86_64 4.19.91-19.1.al7.x86_64 4.19.91-21.al7.x86_64 4.19.91-22.2.al7.x86_64

References

Enable web tamper proofing

Enable the web tamper proofing feature

View the protection status

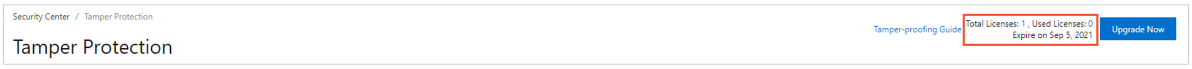
Add blocked processes to a whitelist

4.2. Enable the web tamper proofing feature

The Basic Anti-Virus, Advanced, and Enterprise editions of Security Center provide the web tamper proofing feature to protect your websites.

Prerequisites

- If you use the Security Center Basic edition and want to use the web tamper proofing feature, you must upgrade Security Center to the Basic Anti-Virus, Advanced, or Enterprise edition.
- The web tamper proofing feature supports Windows 32-bit, Windows 64-bit, and Linux 64-bit. If you use an operating system that is supported by this feature, the directories, the file sizes, and the number of files that can be protected are not limited. For more information about the supported system and kernel versions, see Limits on versions of operating systems and kernels. For an operating system that is not supported by this feature, limits are imposed on the directories and files that can be protected. For more information, see Limits.
- Before you use the web tamper proofing feature, make sure that you have sufficient licenses under your account. One license allows you to enable this feature for one server. The number of used licenses equals the number of servers for which this feature is enabled. In the upper-right corner of the **Tamper Protection** page, you can view the total licenses, used licenses, and license expiration date. The expiration date of a web tamper proofing license is the same as that of Security Center. You can purchase additional **licenses** as needed. For more information, see Purchase licenses.


Security Center / Tamper Protection

Tamper Protection

Total Licenses: 1 , Used Licenses: 0
Expire on Sep 5, 2021

> Note Make sure that you use the licenses before they expire. A license becomes invalid after it expires. You cannot request a refund for invalid licenses.

Context

- After you purchase sufficient web tamper proofing licenses, you can enable this feature for servers and directories as needed.
- Tamper protection does not take effect immediately after you configure the protected directory, and you can still write files to the directory. In this case, you must go to the **Management** page, disable **Protection** for the server where the directory is located, and then enable **Protection** again.

  > Note For more information about how to turn on **Protection**, see .

Limits

- For each server, you can enable the web tamper proofing feature for a maximum of 10 directories.
- Limits on the directories that you want to protect in Windows and Linux systems are the same.
  - The maximum size of a directory is 20 GB.
  - The maximum number of folders in a directory is 20,000.
  - The maximum number of directory levels is 20.
  - The maximum size of a file is 20 GB.
- If no licenses are available, you cannot enable the web tamper proofing feature for a new server. If a

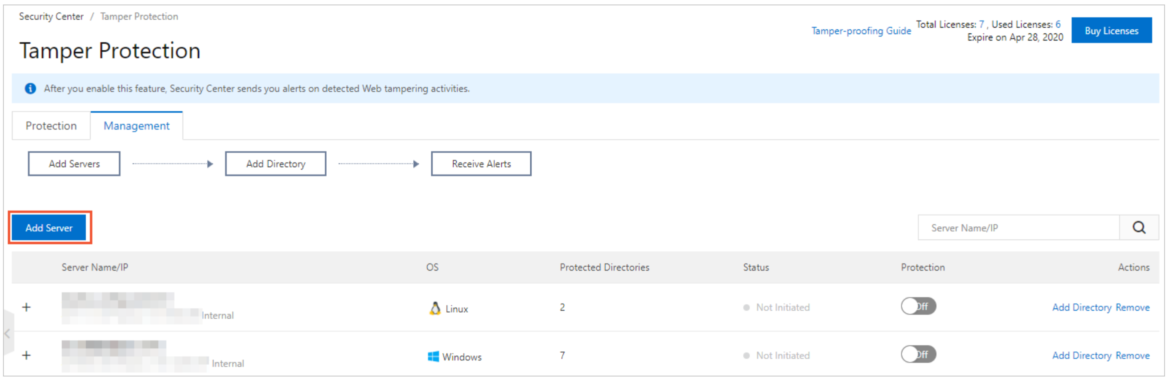
server no longer requires this feature, you can turn off **Protection** to release the license. You can use the released license to enable this feature for a new server.

Note

- Limits on the directories, the file sizes, and the number of files that can be protected are applicable only to the servers whose operating system and kernel versions are not supported by this feature. For more information about the supported system and kernel versions, see Limits on versions of operating systems and kernels.
- Before you enable the web tamper proofing feature, make sure that the directory level, number of folders, and directory size meet the preceding requirements.
- We recommend that you exclude file formats that do not require protection, such as *LOG*, *PNG*, *JPG*, *MP4*, *AVI*, and *MP3*. Separate multiple file formats with semicolons (;).

Procedure

1.
2.
3.
4. On the **Management** tab, click **Add Server** to enable the web tamper proofing feature for a server.



Security Center / Tamper Protection

Tamper Protection

Tamper-proofing Guide Total Licenses: 7 , Used Licenses: 6 Expire on Apr 28, 2020 Buy Licenses

After you enable this feature, Security Center sends you alerts on detected Web tampering activities.

Protection Management

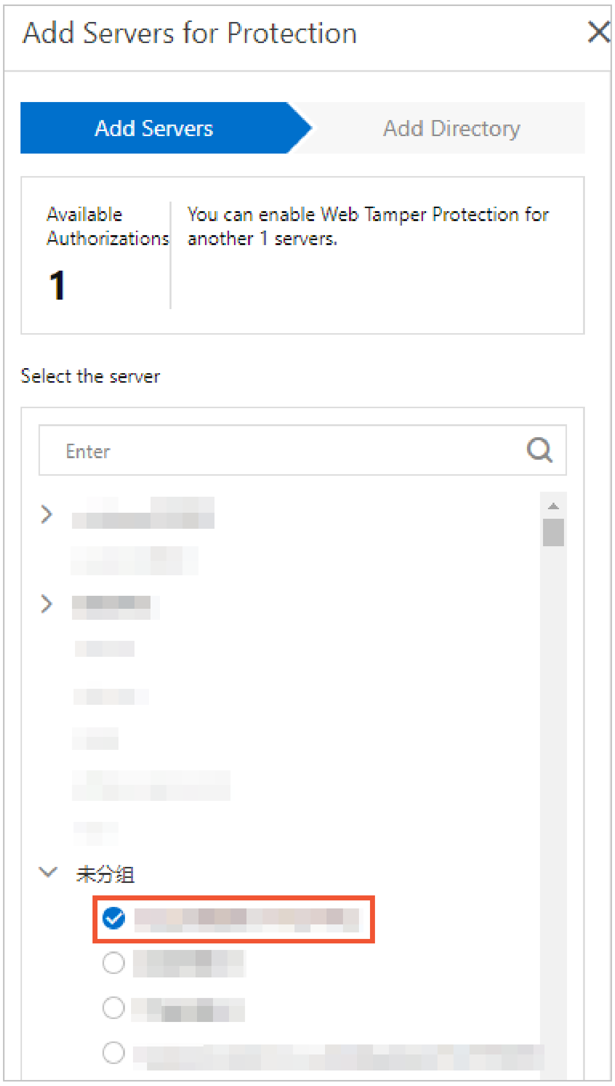
Add Servers → Add Directory → Receive Alerts

Add Server

Server Name/IP

	Server Name/IP	OS	Protected Directories	Status	Protection	Actions
+	[redacted] Internal	Linux	2	Not Initiated	Off	Add Directory Remove
+	[redacted] Internal	Windows	7	Not Initiated	Off	Add Directory Remove

5. In the Add Servers step of the **Add Servers for Protection** wizard, select a server that you want to protect.



Add Servers for Protection

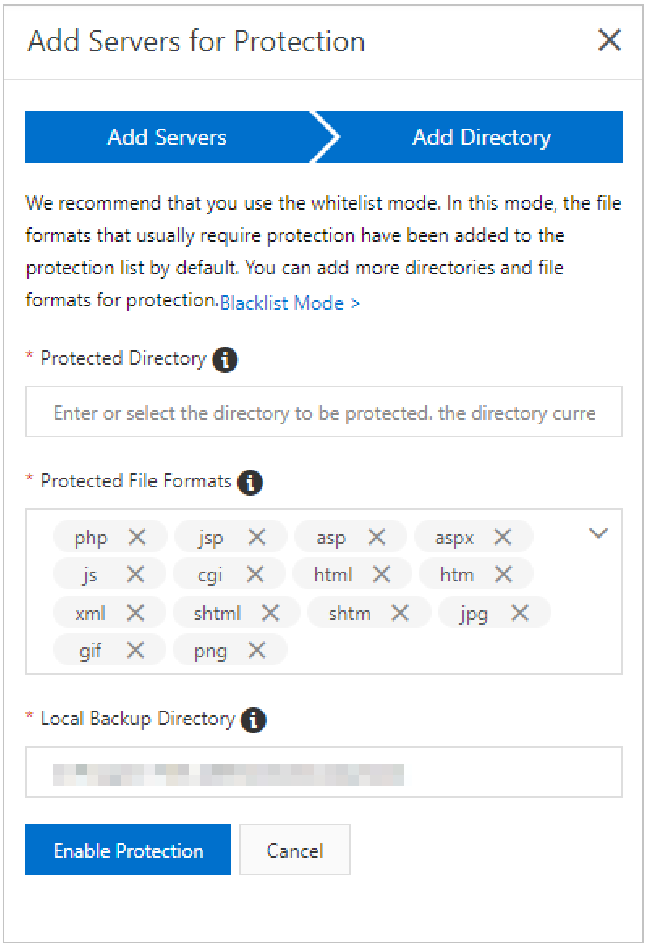
Available Authorizations 1

You can enable Web Tamper Protection for another 1 servers.

Select the server

Note If no licenses are available, you cannot enable the web tamper proofing feature for a new server. If a server no longer requires this feature, you can turn off **Protection** to release the license. You can use the released license to enable this feature for a new server.

6. Click **Next** to go to the **Add Directory** step.
7. In the **Add Directory** step, configure the parameters.



We recommend that you use the whitelist mode. In this mode, the file formats that usually require protection have been added to the protection list by default. You can add more directories and file formats for protection.Blacklist Mode >

* Protected Directory

Enter or select the directory to be protected. the directory curre

* Protected File Formats

php jsp asp aspx js cgi html htm xml shtml shtm jpg gif png

* Local Backup Directory

[redacted]

Select a protection mode. You can select **Whitelist Mode** or **Blacklist Mode**. In whitelist mode, this feature is enabled for the specified directory and file formats. In blacklist mode, this feature is enabled for the subdirectories, file formats, and files that are not excluded. By default, the whitelist mode is used.

- Whitelist mode

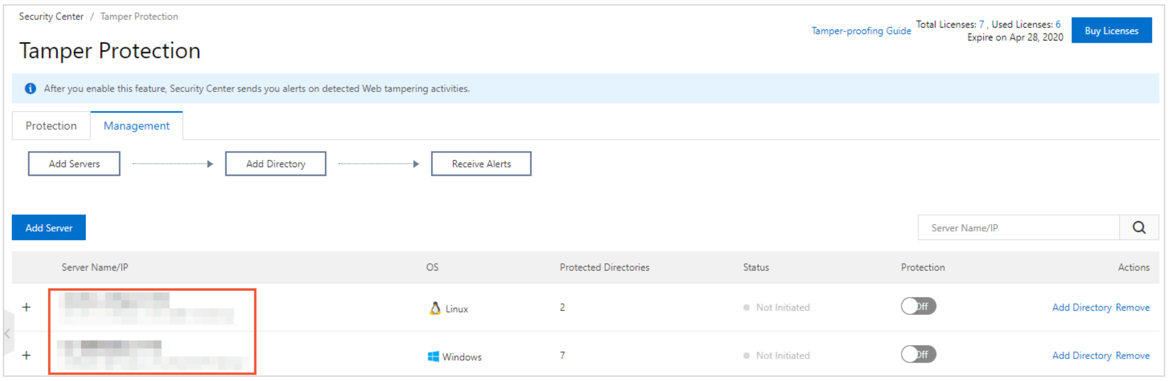
Parameter	Description
Protected Directory	Enter the path of the directory that you want to protect. Note Servers that run Linux and Windows operating systems use different path formats. Enter the correct directory path based on your operating system.
Protected File Formats	Select file formats that you want to protect from the drop-down list, such as *js*, *html*, *xml*, and *jpg*.
Local Backup Directory	The default path where the backup files of the protected directory are stored. By default, Security Center assigns */usr/local/aegis/bak* as the backup path for servers that run Linux operating systems and *C:\Program Files (x86)\Alibaba\Aegis\bak* for servers that run Windows operating systems. You can modify the default path as needed.

- Blacklist mode

Parameter	Description
Protected Directory	Enter the path of the directory that you want to protect.
Excluded Sub-Directories	Enter the path of the subdirectory for which you do not need to enable this feature. You can click **Add Sub-Directory** to add multiple subdirectories. The files under the excluded subdirectories are not protected by Security Center.
Excluded File Formats	Select the formats of files for which you do not need to enable this feature. Valid values: **log**, **txt**, and **ldb**. The files of the specified formats are not protected by Security Center.
Excluded Files	Enter the path of the file for which you do not need to enable this feature. You can click **Add File** to add multiple paths. The files in the specified paths are not protected by Security Center.
Local Backup Directory	The default path where the backup files of the protected directory are stored. By default, Security Center assigns */usr/local/aegis/bak* as the backup path for servers that run Linux operating systems and *C:\Program Files (x86)\Alibaba\Aegis\bak* for servers that run Windows operating systems. You can modify the default path as needed.

8. Click **Enable Protection**.
   After you enable this feature for a server, the server is displayed in the server list on the Management tab of the **Tamper Protection** page.

   > **Note** By default, **Protection** is turned off for the new server. To use the web tamper proofing feature, you must turn on **Protection** of the server on the Management tab of the **Tamper Protection** page.



Security Center / Tamper Protection

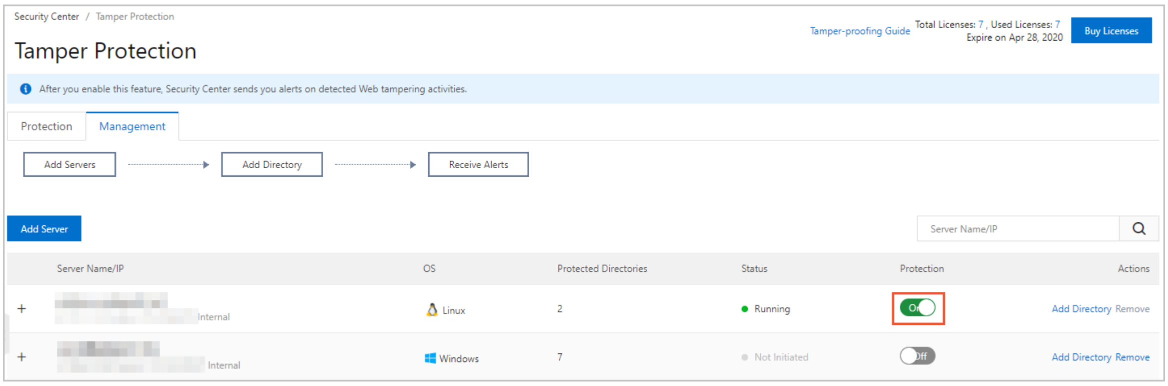
Tamper Protection

Tamper-proofing Guide Total Licenses: 7 , Used Licenses: 6 Expire on Apr 28, 2020 Buy Licenses

After you enable this feature, Security Center sends you alerts on detected Web tampering activities.

	Server Name/IP	OS	Protected Directories	Status	Protection	Actions
+	[redacted]	Linux	2	Not Initiated	Off	Add Directory Remove
+	[redacted]	Windows	7	Not Initiated	Off	Add Directory Remove

9. In the server list, turn on **Protection** to enable this feature for the new server.



Security Center / Tamper Protection

Tamper Protection

Tamper-proofing Guide Total Licenses: 7 , Used Licenses: 7 Expire on Apr 28, 2020 Buy Licenses

After you enable this feature, Security Center sends you alerts on detected Web tampering activities.

Protection Management

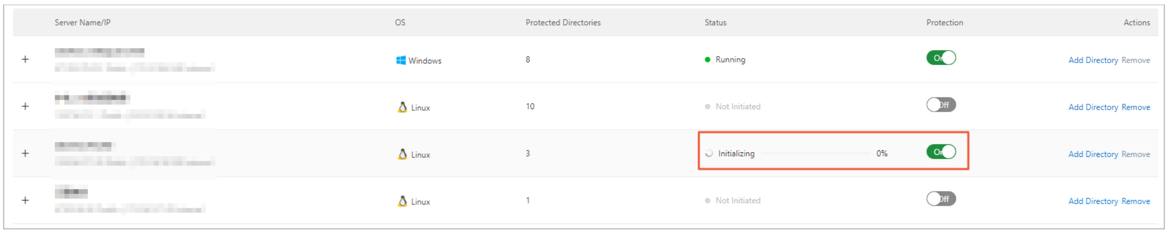
Add Servers → Add Directory → Receive Alerts

Add Server Server Name/IP

	Server Name/IP	OS	Protected Directories	Status	Protection	Actions
+	[redacted] Internal	Linux	2	● Running	On	Add Directory Remove
+	[redacted] Internal	Windows	7	● Not Initiated	Off	Add Directory Remove

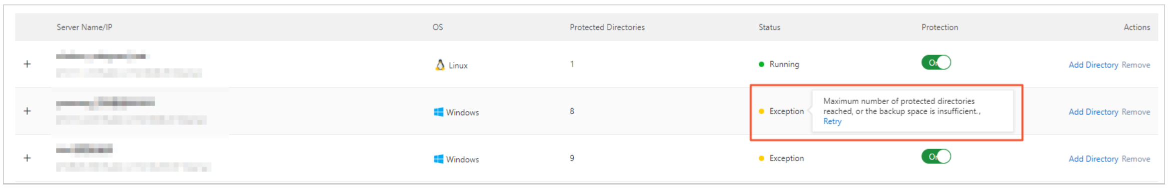
> **Note** By default, **Protection** is turned off for the new server. To use the web tamper proofing feature, you must turn on Protection of the server on the Management tab of the **Tamper Protection** page.

If this is the first time you enable this feature for a server, the status of the server is **Initializing**, and a progress bar appears. It requires a few seconds to enable this feature. After this feature is enabled, the status changes to **Running**.



	Server Name/IP	OS	Protected Directories	Status	Protection	Actions
+	[redacted]	Windows	8	● Running	On	Add Directory Remove
+	[redacted]	Linux	10	● Not Initiated	Off	Add Directory Remove
+	[redacted]	Linux	3	Initializing 0%	On	Add Directory Remove
+	[redacted]	Linux	1	● Not Initiated	Off	Add Directory Remove

If the status of a server is **Exception**, move the pointer over **Exception** in the Status column. A message that indicates the causes appears. Click **Retry** in the message.

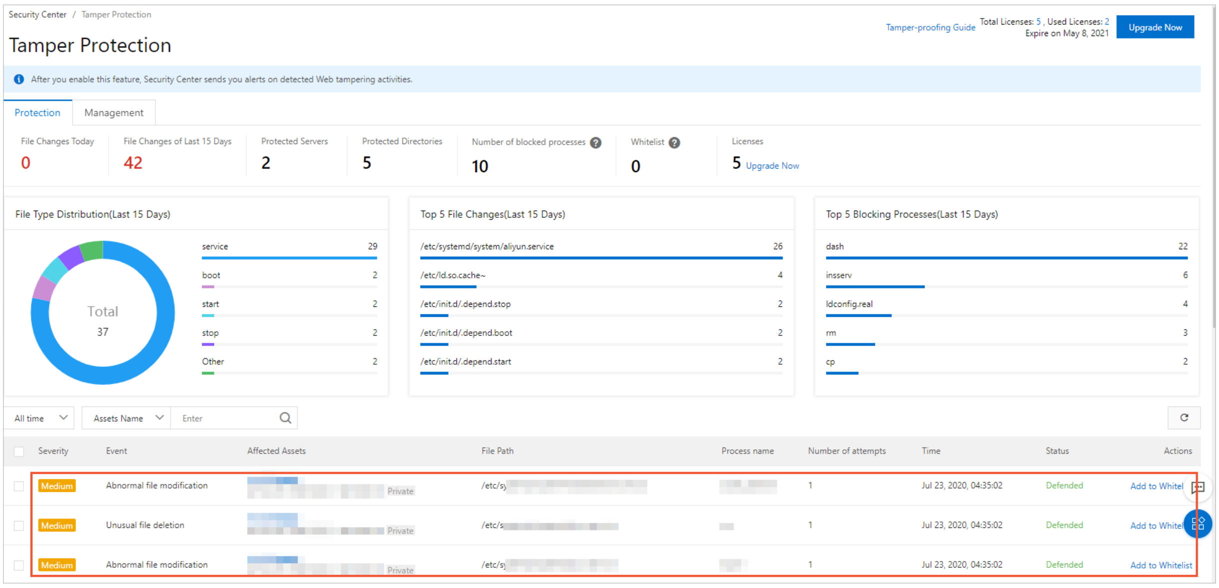


	Server Name/IP	OS	Protected Directories	Status	Protection	Actions
+	[redacted]	Linux	1	● Running	On	Add Directory Remove
+	[redacted]	Windows	8	● Exception		Add Directory Remove
+	[redacted]	Windows	9	● Exception	On	Add Directory Remove

Maximum number of protected directories reached, or the backup space is insufficient., Retry

What to do next

After you enable this feature for a server, go to the **Tamper Protection** page to view detected web tampering events and alerts.



Tamper Protection

Total Licenses: 5 , Used Licenses: 2
Expire on May 8, 2021

After you enable this feature, Security Center sends you alerts on detected Web tampering activities.

File Changes Today	File Changes of Last 15 Days	Protected Servers	Protected Directories	Number of blocked processes	Whitelist	Licenses
0	42	2	5	10	0	5 Upgrade Now

File Type Distribution(Last 15 Days)

Total 37

service	29
boot	2
start	2
stop	2
Other	2

Top 5 File Changes(Last 15 Days)

/etc/systemd/system/aliyun.service	26
/etc/ld.so.cache~	4
/etc/init.d/.depend.stop	2
/etc/init.d/.depend.boot	2
/etc/init.d/.depend.start	2

Top 5 Blocking Processes(Last 15 Days)

dash	22
insserv	6
ldconfig.real	4
rm	3
cp	2

Severity	Event	Affected Assets	File Path	Process name	Number of attempts	Time	Status	Actions
Medium	Abnormal file modification	[redacted] Private	/etc/sy[redacted]	[redacted]	1	Jul 23, 2020, 04:35:02	Defended	Add to Whitel
Medium	Unusual file deletion	[redacted] Private	/etc/s[redacted]	[redacted]	1	Jul 23, 2020, 04:35:02	Defended	Add to Whitel
Medium	Abnormal file modification	[redacted] Private	/etc/sy[redacted]	[redacted]	1	Jul 23, 2020, 04:35:02	Defended	Add to Whitelist

Note Tamper protection does not take effect immediately after you configure the protected directory, and you can still write files to the directory. In this case, you must go to the **Management** page, disable **Protection** for the server where the directory is located, and then enable **Protection** again.

Web tamper proofing states

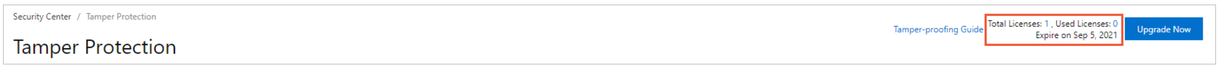
State	Description	Suggestion
Initializing	The web tamper proofing is being initialized.	If this is the first time you enable this feature for a server, the status of the server is **Initializing**. It requires a few seconds to enable this feature.
Running	The web tamper proofing feature is enabled and running as expected.	None.
Exception	An error occurred when you enable the web tamper proofing feature.	Move the pointer over Exception, view the causes, and then click **Retry**.
Not Initiated	The web tamper proofing feature is disabled.	To enable this feature for a server, you must turn on **Protection**.

4.3. Purchase licenses

After you enable tamper protection for a server, one license is consumed. If no license is available, you must purchase more licenses before you can enable tamper protection for other servers. This topic describes how to purchase tamper protection licenses.

Context

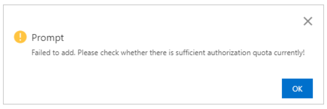
In the upper-right corner of the Tamper Protection page, you can view the total number of licenses, the number of used licenses, and the license expiration date.


Security Center / Tamper Protection

Tamper Protection

Total Licenses: 1 , Used Licenses: 0
Expire on Sep 5, 2021

If no license is available, the **The number of machines has reached the upper limit** message appears. To enable tamper protection for more servers, you must purchase more licenses.

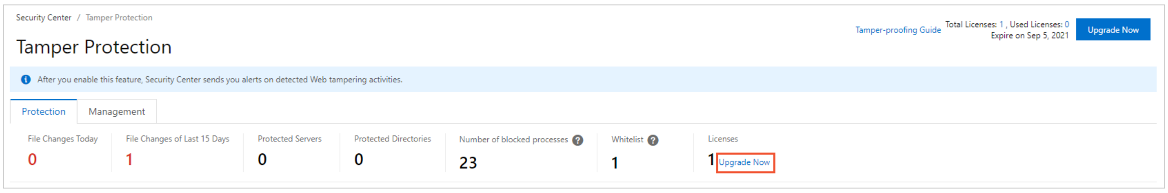

Prompt

Failed to add. Please check whether there is sufficient authorization quota currently!

Procedure

1.
2.
3. In the upper-right corner of the Tamper Protection page, click **Upgrade Now**.

   You can also perform the following steps to purchase more licenses: In the **Protection** section on the Tamper Protection page, click **Upgrade Now** below **Licenses**.

   
   Security Center / Tamper Protection

   Tamper Protection

   Total Licenses: 1 , Used Licenses: 0
   Expire on Sep 5, 2021

   After you enable this feature, Security Center sends you alerts on detected Web tampering activities.

File Changes Today	File Changes of Last 15 Days	Protected Servers	Protected Directories	Number of blocked processes	Whitelist	Licenses
0	1	0	0	23	1	1 Upgrade Now

4. On the **Change Specification** page, specify the number of licenses you want to purchase in the **Web Tamper Protection** section.

   > **Notice** Make sure that the number you specify in the **Web Tamper Protection** section equals the sum of the number of licenses that you have already purchased and the number of licenses that you want to purchase. For example, if you have already purchased five licenses and want to purchase two more, specify seven in the **Web Tamper Protection** section. Unit price: USD 142.6/license/month. The expiration date of the newly purchased licenses is the same as that of the licenses that you have already purchased.

5. Click **Buy Now** and complete the payment.

What's next

After the payment is completed, you can enable web tamper protection for more servers. For more information, see Enable the web tamper proofing feature.

4.4. View the protection status

The web tamper proofing feature monitors changes of directories and files in real time and blocks suspicious file changes. On the Tamper Protection page, you can view the status and details of web tamper proofing for your servers. This topic describes how to view the status of web tamper proofing for your servers.

Prerequisites

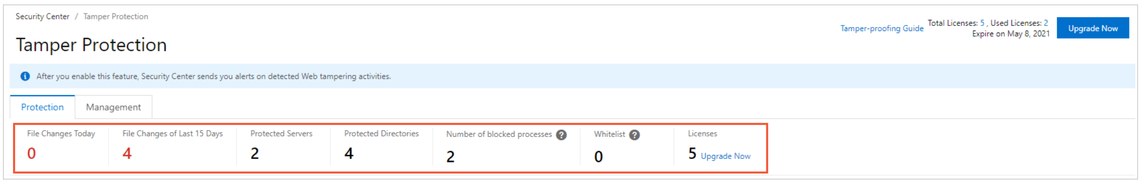
The web tamper proofing feature is enabled to protect your servers. For more information, see Enable web tamper proofing and Enable the web tamper proofing feature.

Procedure

1.
2.
3. On the **Protection** tab, view the details of web tamper proofing for your servers.

   You can view the following web tamper proofing items:

   - Statistical items

     Security Center / Tamper Protection

     Tamper Protection

     Tamper-proofing Guide Total Licenses: 5 , Used Licenses: 2 Expire on May 8, 2021 Upgrade Now

     After you enable this feature, Security Center sends you alerts on detected Web tampering activities.

     Protection | Management

File Changes Today	File Changes of Last 15 Days	Protected Servers	Protected Directories	Number of blocked processes	Whitelist	Licenses
0	4	2	4	2	0	5 Upgrade Now

     In the statistics overview module, you can view the total number of changed files on the current day and in the last 15 days, the number of protected servers and directories, the number of suspicious processes blocked by web tamper proofing, the number of processes in a whitelist, the total number of web tamper proofing licenses purchased for your current account.

   - Distribution of protected file types

     Protected file types include TXT, PNG, MSI, and ZIP. You can also add more types of files for protection as required.

     > Note All types of files can be added for web tamper proofing.

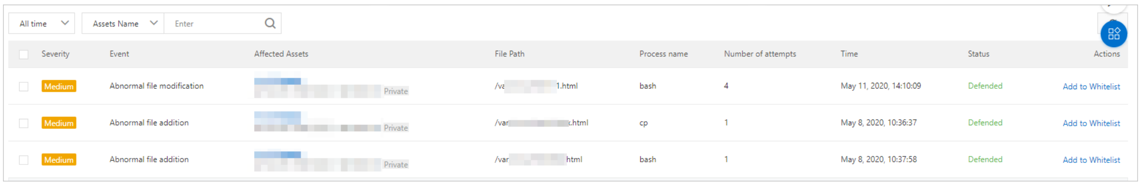
   - Top five files with the largest number of changes

     This module shows the names and paths of the five files with the largest number of changes in the last 15 days.

   - Top five suspicious processes that are blocked

     This module displays the five suspicious processes that are most frequently blocked by web tamper proofing in the last 15 days.

   - Details of web tamper proofing alerts

     All time | Assets Name | Enter

□	Severity	Event	Affected Assets	File Path	Process name	Number of attempts	Time	Status	Actions
□	Medium	Abnormal file modification	[redacted] Private	/va[redacted]1.html	bash	4	May 11, 2020, 14:10:09	Defended	Add to Whitelist
□	Medium	Abnormal file addition	[redacted] Private	/var[redacted].html	cp	1	May 8, 2020, 10:36:37	Defended	Add to Whitelist
□	Medium	Abnormal file addition	[redacted] Private	/var[redacted]html	bash	1	May 8, 2020, 10:37:58	Defended	Add to Whitelist

     The web tamper proofing feature helps you block all suspicious changes to files on your servers. On the alert details page, you can view the alerts of these changes, including the severity, alert name, affected servers, changed directories, suspicious process name, and protection status.

Note

- If the number of alerts exceeds 100, we recommend that you process these alerts at your earliest opportunity.
- Only the alerts at the **Medium** level are displayed in the console.
- Only alerts in the **Defended** state are displayed. This indicates that the web tamper proofing feature has blocked the suspicious processes that attempted to make unauthorized file changes. If the blocked process is required in your workloads, you can add the process to a whitelist of web tamper proofing to enable it. For more information, see Add blocked processes to a whitelist.

4.5. Add blocked processes to a whitelist

If suspicious processes attempt to make unauthorized file changes, the feature of web tamper proofing detects the changes and blocks the processes in real time. If the blocked processes are required in your workloads, you can add the processes to the whitelist of web tamper proofing to allow the processes to be executed. This topic describes how to add the processes that are blocked by web tamper proofing to the whitelist.

Context

Web tamper proofing allows you to add multiple normal processes to the whitelist at a time. You can add blocked processes to the whitelist on Windows and Linux servers.

Limits

You can add blocked processes to the whitelist and enable the alerting mode of web tamper proofing only if your server runs the required OS and kernel. If the versions of the OS and kernel do not meet the requirements, you cannot add blocked processes to the whitelist or enable the alerting mode of web tamper proofing. The following table describes the versions of the OS and kernel.

OS version	Kernel version
CentOS 6.3 CentOS 6.5 CentOS 6.6 CentOS 6.7 CentOS 6.8 CentOS 6.9 CentOS 6.10 CentOS 7.0-1406 CentOS 7.1-1503 CentOS 7.2-1511 CentOS 7.3-1611 CentOS 7.4-1708 CentOS 7.5-1804 CentOS 7.6-1810 CentOS 7.7-1908 CentOS 7.8-2003 CentOS 7.9-2009	2.6.32-**, which indicates all the CentOS kernels whose version numbers start with 2.6.32 3.10.0-**, which indicates all the CentOS kernels whose version numbers start with 3.10.0
CentOS 8.0-1905 CentOS 8.1-1911 CentOS 8.2-2004 CentOS 8.3-2011	4.18.0-80.11.2.el8_0.x86_64 4.18.0-147.5.1.el8_1.x86_64 4.18.0-147.8.1.el8_1.x86_64 4.18.0-193.el8.x86_64 4.18.0-193.6.3.el8_2.x86_64 4.18.0-193.28.1.el8_2.x86_64 4.18.0-240.1.1.el8_3.x86_64 4.18.0-240.15.1.el8_3.x86_64
Ubuntu 14.04	3.13.0-32-generic 3.13.0-65-generic 3.13.0-86-generic 3.13.0-145-generic 3.13.0-164-generic 3.13.0-170-generic 3.19.0-80-generic 4.4.0-93-generic

OS version	Kernel version
Ubuntu 16.04	• 4.4.0-62-generic • 4.4.0-63-generic • 4.4.0-93-generic • 4.4.0-117-generic • 4.4.0-142-generic • 4.4.0-151-generic • 4.4.0-154-generic • 4.4.0-157-generic • 4.4.0-174-generic • 4.4.0-178-generic • 4.4.0-179-generic • 4.4.0-184-generic • 4.4.0-194-generic
Ubuntu 18.04	• 4.15.0-23-generic • 4.15.0-42-generic • 4.15.0-45-generic • 4.15.0-52-generic • 4.15.0-70-generic • 4.15.0-88-generic • 4.15.0-91-generic • 4.15.0-109-generic • 4.15.0-112-generic • 4.15.0-121-generic • 4.15.0-124-generic
AliyunOS 2.1903	• 4.19.81-17.al7.x86_64 • 4.19.81-17.2.al7.x86_64 • 4.19.91-18.al7.x86_64 • 4.19.91-19.1.al7.x86_64 • 4.19.91-21.al7.x86_64 • 4.19.91-22.2.al7.x86_64

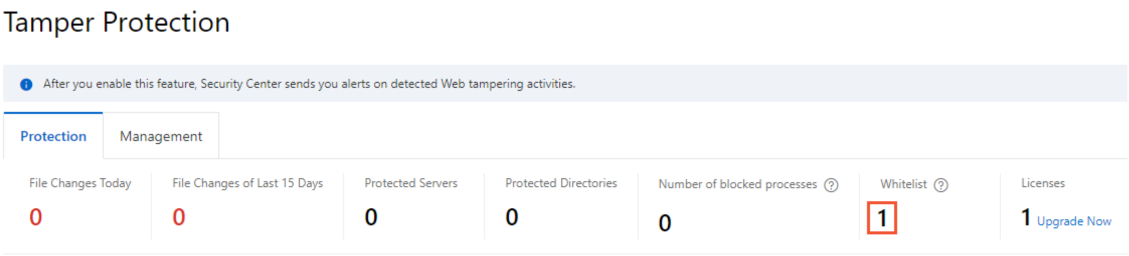
Add blocked processes to a whitelist

1. Log on to the Security center console.
2. In the left-side navigation pane, choose **Defense > Tamper Protection**.
3. On the **Protection** tab of the page that appears, view or search for the suspicious processes for which alerts are generated and that you want to add to the whitelist.
4. Add the suspicious processes to the whitelist.

> **Warning** Attackers may exploit the processes in the whitelist to compromise your servers. We recommend that you add processes to the whitelist only if the processes are trusted.

- **Add a suspicious process for which an alert is generated to the whitelist**
  a. In the alert event list on the Protection tab, find the suspicious process that you want to add to the whitelist.
  b. In the **Actions** column, click **Process**.
  c. In the dialog box that appears, select **Add to Whitelist** for **Process Method**.
  A process may run on multiple servers or run in multiple directories on the same server. If you want to add the process to the whitelist, select **Process servers with the same process at the same time**.
  d. Click **Process Now**.
- **Add multiple suspicious processes for which alerts are generated to the whitelist at a time**
  a. In the alert event list on the Protection tab, find the suspicious processes that you want to add to the whitelist.
  b. Click **Add to Whitelist** below the list.
  c. Click **OK**.

You can click the number below **Whitelist** to go to the **Process Management** panel. In the upper-right corner of the panel, click **Enter the whitelist**. In the dialog box that appears, configure **Process Path** and **Server Name/IP** to add multiple suspicious processes to the whitelist at a time.



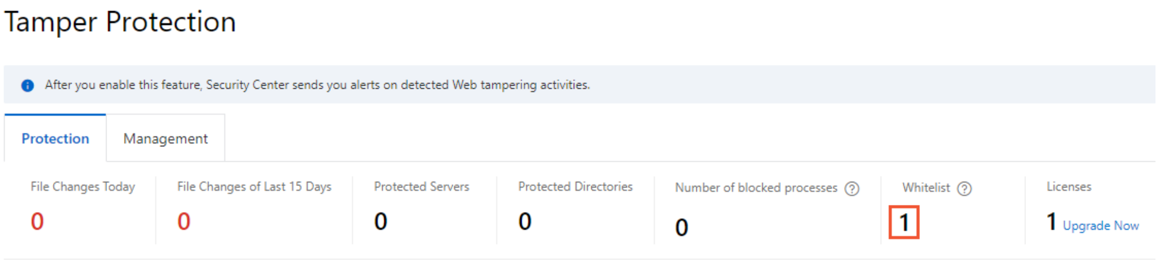
Tamper Protection

After you enable this feature, Security Center sends you alerts on detected Web tampering activities.

File Changes Today	File Changes of Last 15 Days	Protected Servers	Protected Directories	Number of blocked processes	Whitelist	Licenses
0	0	0	0	0	1	1 Upgrade Now

View the processes in the whitelist or remove the processes from the whitelist

1. Log on to the Security center console.
2. In the left-side navigation pane, choose **Defense > Tamper Protection**.
3. On the Protection tab, click the number below **Whitelist**.



Tamper Protection

After you enable this feature, Security Center sends you alerts on detected Web tampering activities.

File Changes Today	File Changes of Last 15 Days	Protected Servers	Protected Directories	Number of blocked processes	Whitelist	Licenses
0	0	0	0	0	1	1 Upgrade Now

4. In the **Process Management** panel, view the processes in the whitelist or remove the processes from the whitelist.

   - **View the processes in the whitelist**
     In the **Process Management** panel, you can view the information about all suspicious processes that are added to the **whitelist**. The information includes the servers on which the processes run, the paths in which the processes are located, and the number of file writing attempts.
   - **Remove the processes from the whitelist**
     In the Process Management panel, you can find the suspicious process that you want to remove and click **Cancel whitelist** in the **Actions** column.
     You can also select multiple suspicious processes and click **Cancel whitelist** below the list to remove these processes from the whitelist at a time.

5.Container firewall feature

5.1. Overview

Security Center provides the container firewall feature. The feature delivers firewall capabilities to protect containers. If attackers exploit vulnerabilities or malicious images to intrude into clusters, the container firewall feature generates alerts or blocks attacks.

How container firewall works

In the container firewall module, network objects are used to identify container applications. The information about a network object includes the namespace to which a container application belongs, the name of the container application, the image of the container that is used to run the container application, and labels. You can create a defense rule to protect a cluster based on network objects. The defense rule can detect and block unusual traffic that is destined for the cluster. For more information about how to configure and use the container firewall feature, see Create a network object, Create a defense rule, Manage the defense status and defense rules of a cluster, and View details on the Protection status tab.

Supported operating system versions

A cluster defense rule can be enabled based on the AliNet plug-in that defends against malicious network behavior. The AliNet plug-in is used to block suspicious network connections, Domain Name System (DNS) hijacking, and brute-force attacks. Before you use the container firewall feature, make sure that your cluster nodes run an operating system whose kernel version is supported by the AliNet plug-in. If your cluster nodes run an operating system whose kernel version is not supported by the AliNet plug-in, the defense rule that you create for your cluster does not take effect. The following table describes the versions and kernel versions of the operating systems that are supported by the AliNet plug-in.

Operating system	Operating system version	Kernel version

Operating system	Operating system version	Kernel version
64-bit Ubuntu	• Ubuntu 14.04 • Ubuntu 16.04 • Ubuntu 18.40 • Ubuntu 20.04	• 3.13.0-32-generic • 3.13.0-86-generic • 4.4.0-104-generic • 4.4.0-117-generic • 4.4.0-124-generic • 4.4.0-142-generic • 4.4.0-146-generic • 4.4.0-151-generic • 4.4.0-170-generic • 4.4.0-174-generic • 4.4.0-179-generic • 4.4.0-184-generic • 4.4.0-185-generic • 4.4.0-62-generic • 4.4.0-63-generic • 4.4.0-93-generic • 4.4.0-96-generic • 4.15.0-23-generic • 4.15.0-42-generic • 4.15.0-45-generic • 4.15.0-52-generic • 4.15.0-54-generic • 4.15.0-72-generic • 4.15.0-96-generic • 4.15.0-109-generic • 4.15.0-106-generic • 4.15.0-111-generic • 4.15.0-118-generic • 4.15.0-1047-gcp • 4.15.0-128-generic • 5.4.0-31-generic • 5.4.0-42-generic • 5.4.0-47-generic • 5.4.0-58-generic • 5.4.0-73-generic

Operating system	Operating system version	Kernel version
64-bit CentOS	CentOS 6.5 CentOS 6.6 CentOS 6.7 CentOS 6.8 CentOS 6.9 CentOS 6.10 CentOS 7.0-1406 CentOS 7.1-1503 CentOS 7.2-1511 CentOS 7.3-1611 CentOS 7.4-1708 CentOS 7.5-1804 CentOS 7.6-1810 CentOS 7.7-1908 CentOS 7.8-2003 CentOS 7.9-2009 CentOS 8.0-1905 CentOS 8.1-1911 CentOS 8.2-2004	2.6.32-**, which indicates all the CentOS kernels whose version numbers start with 2.6.32 3.10.0-**, which indicates all the CentOS kernels whose version numbers start with 3.10.0 4.18.0-**, which indicates all the CentOS kernels whose versions are 4.18.0-240.15.1 or earlier 5.4.42-200.el7.x86_64
64-bit Alibaba Cloud Linux	Alibaba Cloud Linux 2.1903	3.10.0-1160.al7.1.x86_64 4.4.95-1.al7.x86_64 4.4.95-3.al7.x86_64 4.19.24-7.al7.x86_64 4.19.24-7.14.al7.x86_64 4.19.81-17.al7.x86_64 4.19.81-17.2.al7.x86_64 4.19.91-19.1.al7.x86_64 4.19.91-21.al7.x86_64 4.19.91-21.2.al7.x86_64 4.19.91-22.al7.x86_64 4.19.91-22.2.al7.x86_64 4.19.91-23.al7.x86_64 4.19.91-24.1.al7.x86_64

5.2. Create a network object

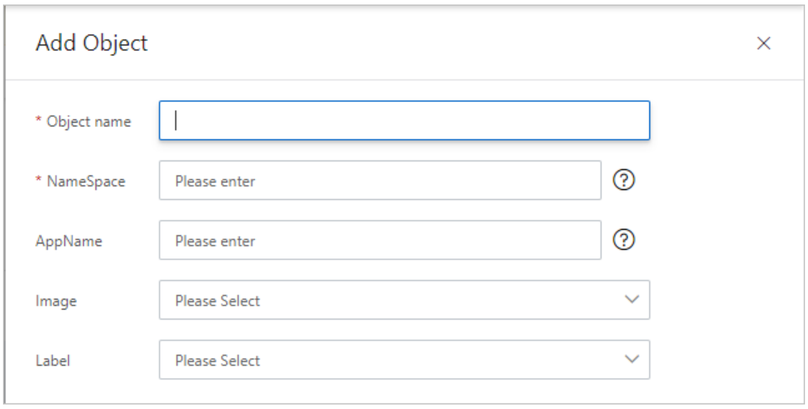
To use the container firewall feature of Security Center, you must create a source network object and a destination network object. This topic describes how to create a network object.

Prerequisites

The behavior prevention feature that defends against malicious network behavior is enabled for your assets. For more information about how to enable the behavior prevention feature, see Use proactive defense.

Procedure

1.
2.
3.
4.
5. In the panel, configure the following parameters.



Add Object

* Object name	
* NameSpace	Please enter
AppName	Please enter
Image	Please Select
Label	Please Select

Parameter	Description
Object name	Enter the name of the network object.
NameSpace	Select or enter the namespace to which the network object belongs. **Note** You can enter the namespace of a cluster. Fuzzy match is supported. Example: a*.
AppName	Select or enter the name of the application to which the network object belongs. **Note** You can enter the label value of a pod whose label key is app. Fuzzy match by suffix is supported. Example: abc*.
Image	Select or enter the image of the network object.
Label	Select or enter the You can select one or more labels. label

6. Click **OK**.
   The new network object appears on the Object tab.
   - You can click **Edit** or **Delete** in the **Operation** column of the network object to modify or delete the network object.

- You can also select multiple network objects and click **Batch delete** below the network object list to delete the network objects at a time.

  > ? **Note** You can delete a network object only when the network object is not added to a defense rule.

What to do next

After you create a source network object and a destination network object, you can create a defense rule to control traffic from the source network object to the destination network object. The defense rule can be used to allow, block, or generate alerts for unusual traffic from the source network object to the destination network object. For more information about how to create a defense rule, see Create a defense rule.

5.3. Create a defense rule

You can create a defense rule to control traffic from a source network object to a destination network object. This topic describes how to create a defense rule.

Context

A defense rule that is created in the container firewall module is used to implement network isolation. A defense rule consists of a source network object, a destination network object, one or more port ranges, an action, and a priority.

Procedure

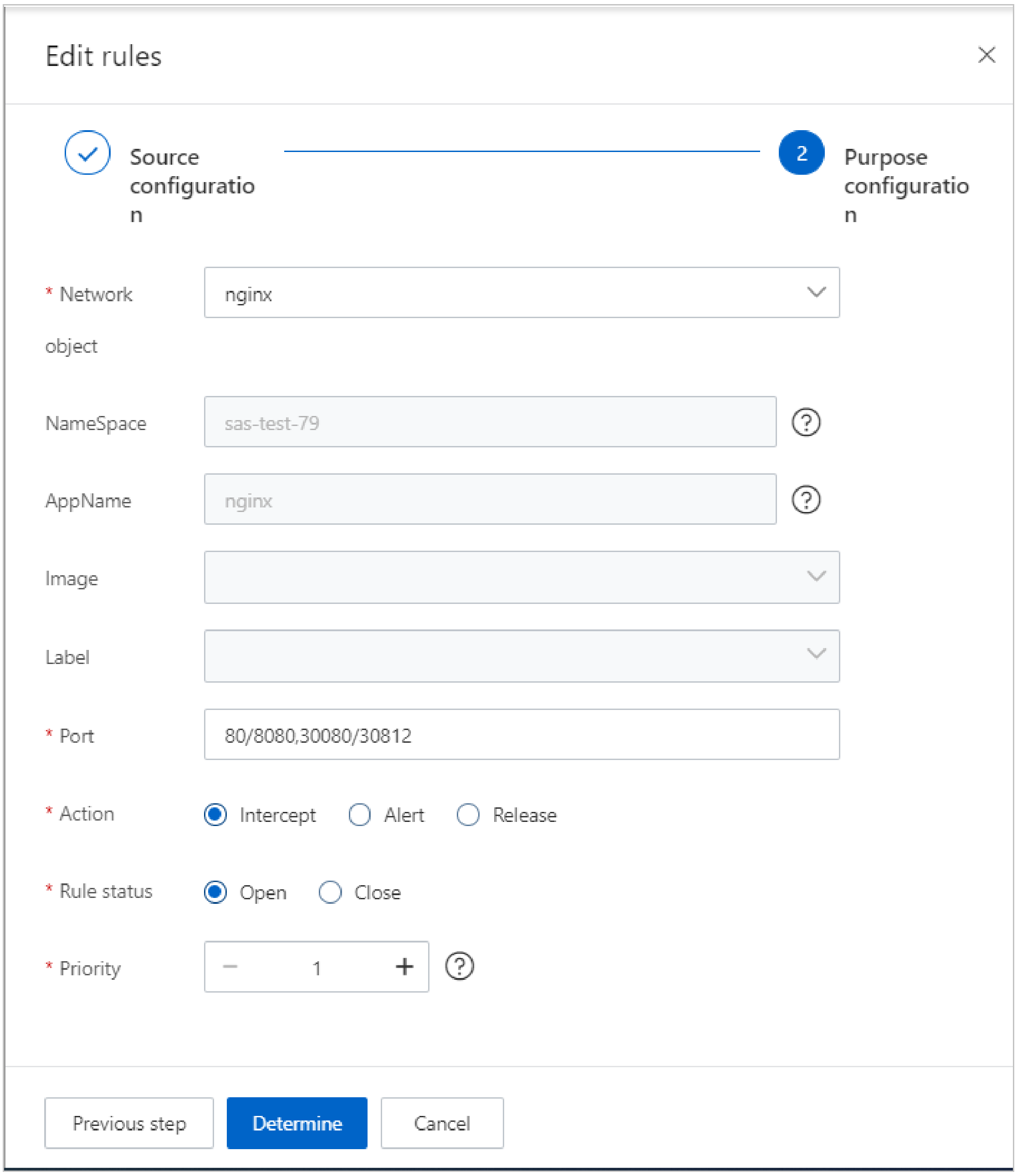
1.
2.
3.
4. In the cluster list of the **Protection management** tab, find the cluster for which you want to create a defense rule and click **Rule management** in the **Operation** column.
5. In the **Defense rules** panel, click **Create rules**.
6. In the **Create rules** panel, create a defense rule for the cluster.
   i. Configure a source network object.

      The following list describes the parameters:

      - Rule name: Enter the name of the defense rule.
      - Network object: Select a source network object as the source of traffic.

   ii. Click **Next**.

   iii. Configure a destination network object.



Edit rules

* Network object: nginx

NameSpace: sas-test-79

AppName: nginx

Image:

Label:

* Port: 80/8080,30080/30812

* Action: ● Intercept ○ Alert ○ Release

* Rule status: ● Open ○ Close

* Priority: 1

The following table describes the parameters.

Parameter	Description
Network object	Select the destination network object as the destination of traffic.
Port	Enter the destination port range of traffic. **Note** You can enter eight port ranges. The port ranges cannot overlap. Separate multiple port ranges with commas (,). Example: 20/30,80/90.

Parameter	Description
Action	Specify the action on traffic. Valid values: ■ **Intercept**: blocks traffic. ■ **Alert**: allows traffic and generates alerts. ■ **Release**: allows traffic and does not generate alerts.
Rule status	Specify the status of the defense rule. Valid values: ■ **Open**: The rule is enabled after it is created. ■ **Close**: The rule is not enabled after it is created.
Priority	Specify the priority of the defense rule. Valid values: 1 to 1000. A smaller value indicates a higher priority.

7. Click **Determine**.
   The defense rules that you create are displayed in the defense rule list in descending order of priority. By default, a newly created defense rule is disabled. You must enable the defense rule to allow the rule to take effect. For information about how to enable a defense rule, see Manage the defense status and defense rules of a cluster.
   After you enable the defense rules of a cluster, the rules are applied in sequence based on the priorities that you specify.

   > **Note** If the traffic from the source network object does not match the first defense rule, the subsequent rules are used until a rule is hit. Then, the hit rule processes traffic based on the action that you specify in the hit rule. If no defense rules are hit, container firewall allows the traffic.

5.4. Manage the defense status and defense rules of a cluster

After you create defense rules for a cluster, you can enable or disable defense for the cluster. You can also enable, disable, and modify the defense rules of the cluster. If you no longer need a defense rule, you can delete it. This topic describes how to enable, disable, modify, and delete a defense rule.

Prerequisites

A defense rule is created for your cluster. For more information about how to create a defense rule, see Create a defense rule.

Context

The defense rule that is created for the cluster can take effect only when the blocking status of the cluster is normal. If the blocking status is abnormal, you must troubleshoot the issue. For more information, see Troubleshoot the issues causing the abnormal blocking status of a cluster.

Manage the defense status

1.
2.
3.
4. In the cluster list of the **Protection management** tab, find the cluster for which you want to manage the defense status.

   Turn on or off ● in the **Defensive status** column to enable or disable defense for the cluster.

   You can also select multiple clusters and click **Batch open** or **Batch shutdown** below the list to manage the defense status for multiple clusters.

   > **Notice** You can enable defense rules for a cluster only when **Normal** is displayed in the **Interceptible status** column of the cluster. If **Abnormal** or **Normal to be confirmed** is displayed in the **Interceptible status** column, you cannot enable defense rules for the cluster. For more information about how to troubleshoot the issues that cause the abnormal status in the **Interceptible status** column, see Troubleshoot the issues causing the abnormal blocking status of a cluster.

Manage a defense rule

1.
2.
3.
4. In the cluster list of the **Protection management** tab, find the cluster whose defense rules you want to manage.

   i. Click **Rule management** in the **Operation** column to go to the **Defense rules** panel.

ii. In the defense rule list of the **Defense rules** panel, find the defense rule that you want to manage.

- Enable or disable the defense rule

  Turn on or off ● in the **Enabled status** column to enable or disable the defense rule.

  You can also select multiple defense rules and click **Batch open** or **Batch shutdown** below the list to enable or disable the defense rules at a time.

- View the details about the defense rule
  Click **Details** in the **Operation** column to go to the **Details** panel. In the panel, view the configurations of the source network object and destination network object, and other details about the defense rule.

- Modify the defense rule
  Click **Edit** in the **Operation** column to go to the **Edit rules** panel. In the panel, modify the defense rule.

  > Note The modification on the defense rule takes effect within 1 minute.

- Delete the defense rule
  Click **Delete** in the **Operation** column to delete the defense rule.
  You can also select multiple defense rules and click **Batch delete** below the list to delete the defense rules at a time.

  > Note The defense rule is deleted within 1 minute.

5.5. View details on the Protection status tab

After you create a defense rule for a cluster and enable the defense rule, the defense rule allows, blocks, or generates alerts for the traffic destined for the cluster. You can view the alerts that are generated by the defense rule on the Protection status tab of the Container Firewall page. This topic describes how to view the details on the Protection status tab.

Context

The Protection status tab displays only the alerts generated by defense rules whose action is set to Intercept or Alert. If the action of a defense rule is set to Release, the defense rule does not generate alerts.

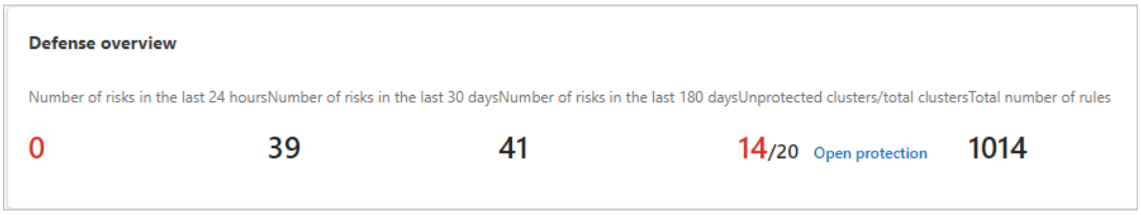
Procedure

1.
2.
3. On the **Container Firewall** page, click the **Protection status** tab.
4. On the **Protection status** tab, view the details.

   The Protection status tab displays defense statistics and the alert list.

   - Defense statistics

You can view the defense statistics in the following sections: **Number of risks in the last 24 hours**, **Number of risks in the last 30 days**, **Number of risks in the last 180 days**, **Unprotected clusters/total clusters**, and **Total number of rules**.



Defense overview

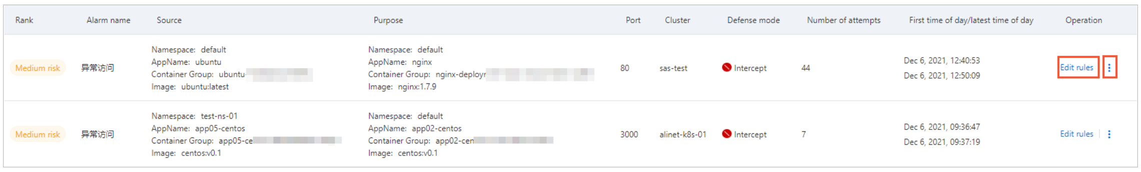
Number of risks in the last 24 hours	Number of risks in the last 30 days	Number of risks in the last 180 days	Unprotected clusters/total clusters	Total number of rules
0	39	41	14/20 Open protection	1014

- Alert list

  You can view the alerts that are sorted by generation time in reverse chronological order. All the alerts are generated by the defense rules whose action is set to Alert or Intercept. If alerts are generated for the same source pod, destination pod, port number, and cluster on the same calendar day, the number of alerts is calculated as 1, and the number of times that access attempts are blocked is displayed in the **Number of attempts** column.

  You can find an alert and click **Edit rules** in the Operation column to modify the action of the defense rule that generated the alert. You can also click the ⋮ icon on the right of **Edit rules** to modify the action of the defense rule.

  Note The modification on the defense rule takes effect within 1 minute.



Rank	Alarm name	Source	Purpose	Port	Cluster	Defense mode	Number of attempts	First time of day/latest time of day	Operation
Medium risk	异常访问	Namespace: default AppName: ubuntu Container Group: ubuntu-[redacted] Image: ubuntu:latest	Namespace: default AppName: nginx Container Group: nginx-deployr[redacted] Image: nginx:1.7.9	80	sas-test	Intercept	44	Dec 6, 2021, 12:40:53 Dec 6, 2021, 12:50:09	Edit rules ⋮
Medium risk	异常访问	Namespace: test-ns-01 AppName: app05-centos Container Group: app05-ce[redacted] Image: centos:v0.1	Namespace: default AppName: app02-centos Container Group: app02-cen[redacted] Image: centos:v0.1	3000	alinet-k8s-01	Intercept	7	Dec 6, 2021, 09:36:47 Dec 6, 2021, 09:37:19	Edit rules ⋮

5.6. Troubleshoot the issues causing the abnormal blocking status of a cluster

If the blocking status of a cluster is Abnormal or Normal to be confirmed, the defense rules that is created for the cluster cannot generate alerts or block unusual traffic destined for the cluster. This topic describes how to troubleshoot the causes of the preceding issues.

Prerequisites

A defense rule is created for your cluster. For more information about how to create a defense rule, see Create a defense rule.

Procedure

1.
2.
3.
4. In the cluster list of the **Protection management** tab, find a cluster whose blocking status is **Abnormal** or **Normal to be confirmed**, and perform the following operations to troubleshoot the issues based on the status:

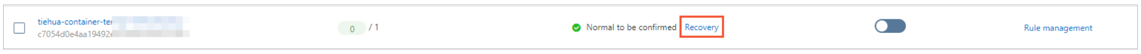
- Abnormal
  If the blocking status in the **Interceptible status** column is **Abnormal**, the switch in the **Defensive status** column is turned off. In this case, Security Center cannot provide the container firewall feature for the cluster.
  You can click **View** on the right of **Abnormal** to go to the **Protection plug-in status** panel. In the **Protection plug-in status** panel, you can check whether the AliNet plug-in is installed in the **Installation status** column and whether the AliNet plug-in is online in the **Online status** column. If the **Installation status** or **Online status** of the AliNet plug-in is abnormal, the blocking status is **Abnormal**. You can perform the following operations to handle the abnormal status in **Installation status** and **Online status**:

  - If the message in the **Installation status** column shows that a cluster node does not have the AliNet plug-in installed, or the message in the **Online status** column shows that the AliNet plug-in on a cluster node is offline, you can enable the behavior prevention feature for the cluster. For more information about how to enable the behavior prevention feature, see Use proactive defense.

  - If you have enabled the behavior prevention feature for the cluster, and the message in the **Installation status** column shows that the cluster node does not have the AliNet plug-in installed, the possible reason is that the kernel version of the operating system that your cluster node runs does not support the AliNet plug-in. .
    You can also log on to the cluster and run the following command to check the installation log of the AliNet plug-in. If the kernel version of the operating system that your cluster node runs does not support the AliNet plug-in, a message `install,driver file not exist` appears in the installation log.

    ```
    cat /usr/local/aegis/PythonLoader/data/alinet_config.log
    ```

- Normal to be confirmed
  If the blocking status in the **Interceptible status** column is **Normal to be confirmed**, you have resolved the issues that cause the **Abnormal** status of the defense rule. In this case, you must check whether all defense rules that are created for the cluster are normal. For example, you can check whether all defense rules are enabled and whether priorities of defense rules are reasonable.
  After you confirm that all defense rules are normal, you can click **Recovery** on the right of **Normal to be confirmed** in the **Interceptible status** column. Then, the blocking status changes to **Normal**.



6.Use malicious behavior defense

Security Center provides the malicious behavior defense feature. You can enable or disable system defense rules, and manage the assets to which each system defense rule is applied based on your business requirements. This topic describes how to use the malicious behavior defense feature.

Limits

Scenarios

- Use system defense rules that are suitable for your business scenarios
  If a system defense rule is not suitable for your business scenarios and affects the security score of your assets, you can disable the rule. For more information, see Manage a system defense rule.
- Handle alerts that are false positives
  If you handle an alert whose alert type is **Precise Defense** and you determine that the processes detected and reported by Security Center based on a system defense rule are normal processes that are required in your workloads, you can disable the rule on the **Host defense rules** tab of the **Malicious behavior Defense** page. You can also remove the affected servers from the list of assets to which the rule is applied. For more information, see Handle alerts that are false positives.

Manage a system defense rule

1.
2.
3.
4. In the list of system defense rules, search for the system defense rule that you want to manage.
   - On the **Host defense rules** tab, enter the name of the system defense rule in the search box.
   - In the left-side navigation pane of the **Host defense rules** tab, select a value in the **ATT&CK Phase** section.
5. Manage a system defense rule.
   - **Enable or disable a rule**

     > **Notice** After you disable a system defense rule, Security Center no longer detects risks or generates alerts based on the rule. The alerts that are generated based on the rule are no longer displayed on the **Alerts** page. Proceed with caution.

     a. Select one or more system defense rules based on your business requirements.
     b. In the lower-left corner of the rule list, click **Enabled** or **Deactivation**.
   - **Manage assets in a rule**

     > **Notice** After you remove an asset from a rule, Security Center no longer detects or reports risks on the asset based on the rule. Proceed with caution.

     a. Select the system defense rule that you want to manage.
     b. Click **Management host** in the **Actions** column.

c. In the **Management host** panel, add the assets to the rule or remove the assets from the rule.

d. Click **OK**.

Handle alerts that are false positives

1.

2.

3. On the **Alerts** page, click the number that is displayed below **Precise Defense**.

4. In the alert list, find the alert that is a false positive and click **Details** in the **Actions** column to view the alert details.

   The following section provides an example on how to handle an alert that is a false positive. In this example, the alert named **Suspicious worm script behavior** is handled.
   On the Alert Details panel, obtain and record the following information for subsequent use.

   - The name of the system defense rule that detects risks and generates alerts. In this example, the system defense rule is **Suspicious worm script behavior**.
   - The value of **ATT&CK Phase** of the alert. In this example, the value is **Impact**.
   - The names and IP addresses of the assets that are affected by the alert.

5. In the left-side navigation pane, click **Malicious behavior Defense**.

6. On the Host defense rules tab, search for the system defense rule that detects risks and generates alerts.

   - You can enter **Suspicious worm script behavior** in the search box.
   - You can also click **Impact** in the **ATT&CK Phase** section on the left side of the Host defense rules tab.

7. In the rule list, find and manage the system defense rule **Suspicious worm script behavior**.

   - If the system defense rule is not suitable for your business scenario and you no longer want Security Center to generate alerts for the risks that are detected by the system defense rule, you can click the icon in the **Switch** column to disable the rule.

     > **Notice** After you disable a system defense rule, Security Center no longer detects risks or generate alerts based on the rule. The alerts that are generated based on the rule are no longer displayed on the Alerts page. Proceed with caution.

   - If you want to handle only an alert that is a false positive, you can click **Management host** in the **Actions** column to remove the assets that are affected from the asset list of the rule.
     You can also go to the **Alerts** page and click **Process** in the **Actions** column of the alert. In the Handle dialog box, select **Disable Malicious Behavior Prevention** and click **Process Now** to handle the alert that is a false positive. After an alert is handled, the assets that are affected by the alert are removed from the asset list of the system defense rule.

     > **Notice** If you want to handle only an alert that is generated based on the system defense rule and you want the system defense rule to continue to protect the asset, you can add the asset to the asset list on the Malicious behavior Defense page.

7.Proactive defense for containers

7.1. Overview

Security Center provides the feature of proactive defense for containers. The feature allows you to detect risks on an image when you use the image to create resources in a cluster. The feature also allows you to create a container defense policy for a cluster. If an image hits the container defense policy, Security Center handles the image that is started in the cluster based on the action of the policy. The action can be Block, Alert, or Allow. This ensures that the image does not affect your business.

Limits

How proactive defense for containers works

After you create a container defense policy for a cluster, a request is sent to Security Center to detect image risks when you use an image to create resources such as pods in the cluster. Security Center detects risks on the image based on the container defense policy. The risks include vulnerabilities, baseline risks, and malicious samples. If the image hits the container defense policy, Security Center handles the image based on the action of the policy, and an alert is generated for the risk detection result. The action can be Alert, Block, or Allow.

For more information about how to configure and use the feature of proactive defense for containers, see Create container defense policies, Manage container defense policies, and View and handle alerts.

Supported ACK clusters

The feature of proactive defense for containers supports the following Container Service for Kubernetes (ACK) clusters.

ACK cluster	Supported
Managed Kubernetes cluster	Yes
Dedicated Kubernetes cluster	Yes
Serverless Kubernetes cluster	No
Managed edge Kubernetes cluster	No
Registered cluster	No

7.2. Create container defense policies

Security Center provides the feature of proactive defense for containers. The feature detects risks on an image in a cluster when the image is started. The feature allows you to create a container defense policy for a cluster. If an image hits the container defense policy, Security Center handles the image based on the action of the policy. The action can be Alert, Block, or Allow. This topic describes how to create a container defense policy for a cluster.

Prerequisites

The policy-template-controller component for security policy management is installed in the Container Service for Kubernetes (ACK) console. For more information, see Install policy-template-controller.

Limits

Create a container defense policy

> ? **Note** You can create up to 40 container defense policies for each cluster.

1.
2. In the left-side navigation pane, choose **Defense > Proactive Defense for Containers**.
3. On the Proactive Defense for Containers page, click the **Policy** tab. In the left-side section of the Policy tab, click a cluster for which you want to create a container defense policy.
4. Click **Create Policy** to go to the **Create Policy** panel.
5. In the **Create Policy** panel, configure the parameters.

   The following table describes the parameters.

Parameter	Description
Policy Template	Select a template to create the policy. You can select Blank template to create a policy based on your business requirements. You can also select an existing template with preconfigured risk detection settings.

Parameter	Description
Unscanned Image	Specify whether to allow the images that are not scanned by container image scan to start. **Note** If you turn on the switch, the images that you specify in the policy are scanned. If you turn on the switch, we recommend that you set Action to **Alert**. If you have high demands for security performance, you can change the action to **Block**. Before you change the action, we recommend that you observe the alerts that are generated based on the current policy and check whether your business is affected. If your business is not affected, you can change the action of the policy.
Malicious Internet Image	Specify whether to block the startup of malicious images that are spread over the Internet. Malicious images include malicious images that are downloaded from public image repositories and the images that are pulled from Docker Hub repositories and contain malicious programs such as webshells and trojans.

Parameter	Description
Alert Policy	Configure the alert policy for the following types of risks: ◦ Baseline ◦ Vulnerability ◦ Malicious Sample You can configure alert policies for baseline risks, vulnerabilities, and malicious samples based on your business requirements. **Notice** ◦ If an alert policy that is configured for a type of risk is matched, Security Center immediately handles the risks based on the action of the container defense policy. The remaining alert policies are no longer matched. Alert policies are matched against the following types of risks in sequence: malicious Internet images, unscanned images, malicious samples, baseline risks, and vulnerabilities. ◦ The optional conditions of an alert policy are evaluated by using a logical OR. If you set Risk Level to **High** and specify **CVE ID** when you configure an alert policy for vulnerabilities, the alert policy is hit if the images that are started in the cluster contain high-risk vulnerabilities or if the images contain vulnerabilities with the specified CVE IDs.
Policy Name	Enter a name for the policy.
Description	Enter a description for the policy.
Namespace	Select the namespace in which images are started. You can select multiple namespaces.
Image	Select an image. You can select multiple images.

Parameter	Description
Tag	Select the tag of an image. You can select multiple tags.
Action	Specify the action of the container defense policy. Valid values: ○ **Alert**: If an image hits the policy, an alert is generated. ○ **Block**: If an image that hits the policy is being started, it is blocked. ○ **Allow**: If an image hits the policy, it is allowed.
Add to Whitelist	Enter the name of the image that you want to add to the whitelist. You can add up to 20 images to the whitelist. Fuzzy match is supported by using keywords. For example, if you want to add the image whose address is yundun-example-registry.cn-hangzhou.aliyuncs.com/yundun-example/yun-repo:test to the whitelist, you can enter one of the following keywords: ○ yun-repo ○ test ○ yun-repo:test ○ repo:test **Notice** After you add an image to the whitelist, Security Center does not detect risks on the image when the image is started. Proceed with caution.

6. Click **OK**.
   After the container defense policy is created, Security Center detects risks on the image that is specified in the policy based on the policy configurations when the image is started. The detection result is displayed as an alert in the alert list.

Create a policy based on an existing policy

1.
2. In the left-side navigation pane, choose **Defense > Proactive Defense for Containers**.
3. On the Proactive Defense for Containers page, click the **Policy** tab. In the left-side section of the Policy tab, click a cluster for which you want to create a container defense policy.
4. In the policy list, find an existing policy and click **Copy** in the **Actions** column to go to the **Copy Policy** panel.
5. In the **Copy Policy** panel, modify the policy parameters based on your business requirements.
6. Click **OK**.
   After the container defense policy is created, Security Center detects risks on the image that is

specified in the policy based on the policy configurations when the image is started. The detection result is displayed as an alert in the alert list.

What to do next

After the policy is created, you can edit and delete the policy based on your business requirements. For more information, see Manage container defense policies.

7.3. Manage container defense policies

After you create a container defense policy, you can edit the policy based on your business requirements. If you no longer require a container defense policy, you can delete the policy. This topic describes how to edit and delete a container defense policy.

Prerequisites

A container defense policy is created. For more information about how to create a container defense policy, see Create container defense policies.

Edit a container defense policy

1.
2. In the left-side navigation pane, choose **Defense > Proactive Defense for Containers**.
3. On the Proactive Defense for Containers page, click the **Policy** tab. In the left-side section of the Policy tab, click the cluster whose container defense policy you want to edit.
4. In the policy list, find an existing policy and click **Edit** in the **Actions** column to go to the **Edit Policy** panel.
5. In the **Edit Policy** panel, modify the parameters based on your business requirements.
6. Click **OK**.
   After the container defense policy is edited, Security Center detects risks on the image that is specified in the policy based on the policy configurations when the image is started. The detection result is displayed as an alert in the alert list.

Delete a container defense policy

Notice If you delete a container defense policy, Security Center no longer detects risks on the image that is specified in the container defense policy based on the policy configurations when the image is started. To ensure the runtime security of containers, we recommend that you do not delete container defense policies unless necessary.

1.
2. In the left-side navigation pane, choose **Defense > Proactive Defense for Containers**.
3. On the Proactive Defense for Containers page, click the **Policy** tab. In the left-side section of the Policy tab, click the cluster whose container defense policy you want to delete.
4. In the policy list, find an existing policy and click **Delete** in the **Actions** column.
5. In the **Are you sure that you want to delete the policy?** message, click **OK**.

7.4. View and handle alerts

If an image that hits a container defense policy for a cluster is started in the cluster, an alert is generated. You can view the alert on the Alert tab of the Proactive Defense for Containers page. To ensure the runtime security of containers, we recommend that you view and handle the alerts in Security Center at the earliest opportunity. This topic describes how to view and handle alerts.

Prerequisites

A container defense policy is created. For more information about how to create a container defense policy, see Create container defense policies.

View alert details

1.
2. In the left-side navigation pane, choose **Defense > Proactive Defense for Containers**.
3. On the Proactive Defense for Containers page, click the **Alert** tab. On the Alert tab, view alert statistics.

   The Alert tab displays the following sections: **Defense Trend**, **Top 10 At-risk Clusters**, and **Alerts**.

   - In the **Defense Trend** section, you can view the most recent defense trend of clusters for which you have created container defense policies in a trend chart.
   - In the **Top 10 At-risk Clusters** section, you can view the top 10 clusters whose container defense policies are most frequently hit.
   - In the **Alerts** section, you can view the details about alerts. The details include policy and image details.
     - In the alert list, click the name of an image in the **Image** column to go to the image details page. You can view and handle the risks that are detected on the image on the details page.

       > **Note** The image details page is provided for an image only after the image is added to Security Center. For more information about how to add images to Security Center, see Add image repositories to Security Center.

     - In the alert list, find an image and click the icon in the **Action** column. In the message that appears, you can view the details of the alert policy in the container defense policy that is used to detect image risks.

       > **Notice** The message contains only the information about a risk that is detected on the image. If you want to start the image, you must handle other risks that are detected on the image. This ensures that no container defense policies are hit when the image is started the next time. For more information, see Handle alerts.

     - In the alert list, find a policy and click **Change Policy** in the **Actions** column to change the action of the policy.

Handle alerts

1.
2. In the left-side navigation pane, choose **Defense > Proactive Defense for Containers**.
3. On the Proactive Defense for Containers page, click the **Alert** tab. On the Alert tab, find the image for which an alert is generated and click the image name in the **Image** column to go to the image details page.

The image details page is provided for an image only after the image is added to Security Center. For more information about how to add images to Security Center, see Add image repositories to Security Center.

4. On the image details page, handle the risks that are detected on the image.

   You must handle all risks on the following tabs: **Image System Vul**, **Image Application Vul**, **Image Baseline Check**, and **Image Malicious Sample**. The risks are detected based on the container defense policy of the cluster to which the image belongs. After the risks are handled, Security Center allows the startup of the image, and the existing containers that run in the cluster do not have security risks.

8.FAQ

This topic provides answers to some frequently asked questions about features of Security Center. The features include anti-ransomware, antivirus, web tamper proofing, and application whitelist.

- Questions about the anti-ransomware feature
  - How do I purchase the anti-ransomware capacity?
  - What is the anti-ransomware feature? Why do I must pay for the anti-ransomware feature?
  - What is the relationship between the anti-ransomware feature and Alibaba Cloud HBR?
  - Is the data backup feature automatically enabled after I purchase the anti-ransomware capacity?
  - After I enable the anti-ransomware feature, the data backup cache occupies a large amount of disk space. How do I clear the cache?
  - After I enable the anti-ransomware feature, the data backup cache occupies a large amount of space of drive C on my server. Can I change the directory in which the data backup cache is stored?
  - What do I do if the anti-ransomware agent consumes excessive server CPU or memory resources?
  - What are the differences between the general anti-ransomware solution and the snapshot feature?
  - What do I do if the anti-ransomware capacity that I purchased is insufficient?
  - What do I do if the status of an anti-ransomware policy is abnormal?
- Questions about the antivirus feature
  - After I purchase the antivirus feature, can the existing features properly run?
- Questions about the web tamper proofing feature
  - If the remaining validity period of Security Center is three years, can I purchase web tamper proofing for one year?
  - Can web tamper proofing protect files of all sizes?
  - If my server stores more than 3 MB of files, can web tamper proofing protect the excessive files that exceed 3 MB? Can web tamper proofing protect files whose total size is not larger than 3 MB?
  - The message "The protection module initialization failed. Check whether other software has blocked the creation of the service" appears when I enable web tamper proofing. Why?
  - What are the requirements for the local backup directory of web tamper proofing?
  - What do I do if I receive a message that indicates that a protected directory is invalid?
  - Why does web tamper proofing remain disabled after I specify a protected directory?
  - Can I write files to a protected directory on a server for which web tamper proofing is configured?
  - After I specify a protected directory, what do I do if web tamper proofing does not immediately take effect?
  - I do not receive alert notifications after I log on to my server over SSH and modify the files that are protected by web tamper proofing. Why?
  - After I enable web tamper proofing, what do I do if the website content and images cannot be modified or updated?
  - What do I do if I receive an email or text message that notifies me of a webshell detected on my server?
- Questions about the container firewall feature
  - My Security Center runs the Enterprise edition. Can I use the container firewall feature?

- Do I need to pay for the container firewall feature?
- After I upgrade my Security Center to the Ultimate edition, does Security Center protect only containers?

How do I purchase the anti-ransomware capacity?

If you use the edition of Security Center, you can go to the Security Center buy page to upgrade Security Center to the , , , or edition, and purchase the anti-ransomware capacity. You can also purchase the edition and purchase the anti-ransomware capacity. For more information, see Enable anti-ransomware.

If you use the , , , or edition, you can change the specifications and purchase a specific amount of anti-ransomware capacity. For more information, see Upgrade and downgrade Security Center. After you purchase the anti-ransomware capacity and grant Security Center the permissions to use your cloud resources, the anti-ransomware feature is automatically enabled.

What is the anti-ransomware feature? Why do I must pay for the anti-ransomware feature?

The anti-ransomware feature is a new feature of Security Center, which provides a general anti-ransomware solution. You must purchase the storage that is used to store backup data.

If you use the , , , or edition, you can change the specifications and purchase a specific amount of anti-ransomware capacity. For more information, see Upgrade and downgrade Security Center. After you purchase the anti-ransomware capacity and grant Security Center the permissions to use your cloud resources, the anti-ransomware feature is automatically enabled.
The general anti-ransomware solution allows you to restore the files that are encrypted by ransomware with a few clicks. The general anti-ransomware solution allows you to back up important directories and files on your servers with a few clicks. We recommend that you purchase 50 GB of anti-ransomware capacity for each server, which costs only USD 2.25 per month.

What is the relationship between the anti-ransomware feature and Alibaba Cloud HBR?

The anti-ransomware feature uses the storage capability provided by Alibaba Cloud Hybrid Backup Recovery (HBR). If you have not activated Alibaba Cloud HBR, it is automatically activated after you purchase the anti-ransomware capacity and grant Security Center the permissions to use Alibaba Cloud HBR. You are not charged when you activate Alibaba Cloud HBR.

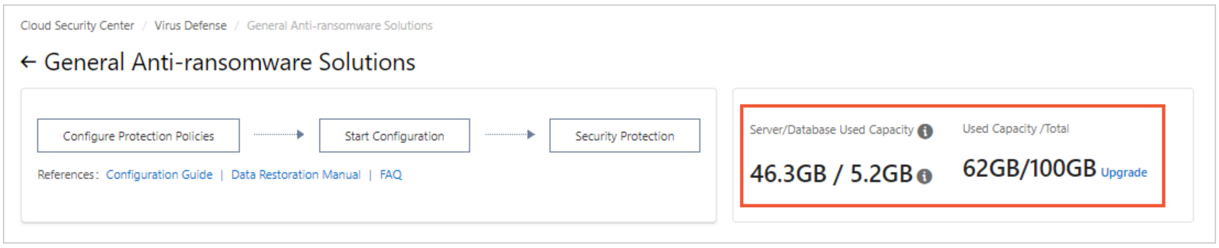
Is the data backup feature automatically enabled after I purchase the anti-ransomware capacity?

No, the data backup feature is not automatically enabled.

After you purchase the anti-ransomware capacity, you must create and enable an anti-ransomware policy. After you enable the anti-ransomware policy, Security Center backs up server data to protect your servers against ransomware.

How do I view the anti-ransomware capacity that I purchased and the anti-ransomware capacity that is used?

After you enable the anti-ransomware feature, you can view the anti-ransomware capacity that you purchased and the anti-ransomware capacity that is used on the **Anti-blackmail** page. To go to the page, choose **Defense > Anti-ransomware** in the left-side navigation pane.


Cloud Security Center / Virus Defense / General Anti-ransomware Solutions
← General Anti-ransomware Solutions
Configure Protection Policies
Start Configuration
Security Protection
References: Configuration Guide | Data Restoration Manual | FAQ
Upgrade

Server/Database Used Capacity: 46.3GB / 5.2GB

Used Capacity /Total: 62GB/100GB

After I enable the anti-ransomware feature, the data backup cache occupies a large amount of disk space. How do I clear the cache?

To accelerate data backup, the anti-ransomware feature caches data during data backup. By default, the data backup cache occupies disk space on your server. If a large amount of disk space is occupied by the cache under the path of *C:\Program Files (x86)\Alibaba\Aegis\hbr\cache* on Windows servers or */usr/local/aegis/hbr/cache* on Linux servers, you can clear the cache. For more information, see Clear backup caches.

After I enable the anti-ransomware feature, the data backup cache occupies a large amount of space of drive C on my server. Can I change the directory in which the data backup cache is stored?

Yes, you can change the directory in which the data backup cache is stored.

You can modify the configuration file of the anti-ransomware agent to change the directory in which the data backup cache is stored. For more information, see Modify backup cache configurations.

What do I do if the anti-ransomware agent consumes excessive server CPU or memory resources?

Earlier versions of the anti-ransomware agent may consume excessive server CPU or memory resources during data backup. This anti-ransomware agent was upgraded on August 19, 2020 to resolve this issue. If you installed the anti-ransomware agent after August 19, 2020, no actions are required. If you installed the anti-ransomware agent on or before August 19, 2020, you must uninstall and reinstall the anti-ransomware agent. To uninstall and reinstall the anti-ransomware agent, perform the following steps:

1. Log on to the .
2. In the left-side navigation pane, choose **Defense > Anti-ransomware**.
3. Find the server on which the issue occurs and click **Uninstall** in the Actions column. In the message that appears, click **OK**.
   Then, the status of the anti-ransomware agent changes to **Uninstalling**. The anti-ransomware agent is uninstalled in about 5 minutes.
4. After the agent is uninstalled, click **Install** in the Actions column. In the message that appears, click **OK**.
   Then, the status of the anti-ransomware agent changes to **Installing**. The anti-ransomware agent is installed in about 5 minutes.

> Note If the issue persists after you perform the preceding steps, we recommend that you to contact Alibaba Cloud technical support.

What are the differences between the general anti-ransomware solution and the snapshot feature?

The following table describes the differences between the general anti-ransomware solution and the snapshot feature.

Feature	Data backup	Antivirus capability	Fee
Snapshot	Provides a one-time backup for the system disk. If you want to restore data, you must restart the system.	The antivirus capability is not provided.	High. The snapshot feature backs up the entire disk. You cannot back up only a specific file. The snapshot feature is charged USD 0.02 per GB per month. For more information, see Snapshots.
General anti-ransomware solution	Flexibly backs up files. You can restore a file that is backed up. If you want to restore data, you do not need to restart the system.	The general anti-ransomware solution blocks known ransomware and generates alerts in real time. This solution captures unknown ransomware and allows you to restore data that is encrypted by ransomware with a few clicks.	Low. The general anti-ransomware solution supports file-level protection. You are charged data backup fees based on your actual usage. You do not need to back up the entire disk. For more information, see Billing.

What do I do if the anti-ransomware capacity that I purchased is insufficient?

If the anti-ransomware capacity that you purchased is insufficient, data backup may fail. You can purchase additional anti-ransomware capacity or release the anti-ransomware capacity.

- Purchase additional anti-ransomware capacity
  Insufficient anti-ransomware capacity causes backup failures. We recommend that you purchase sufficient anti-ransomware capacity to prevent backup failures. To purchase sufficient anti-ransomware capacity, perform the following operations: Log on to the and choose **Defense > Anti-ransomware** in the left-side navigation pane. On the **Anti-blackmail** page, click **Upgrade** below **Used Capacity/Total**.

  > **Note** We recommend that you purchase 50 GB of anti-ransomware capacity for each server.

- Release the anti-ransomware capacity
  - Remove servers
    You can release anti-ransomware capacity by removing servers such as test servers and idle servers from an anti-ransomware policy. For more information, see Manage servers that are added to an anti-ransomware policy.
  - Add directories that you want to protect based on your business requirements
    You can create **custom anti-ransomware policies** and back up only the directories that you want to protect. This helps reduce the amount of anti-ransomware capacity that is used.

- Delete backup data
  If you no longer require backup data of a server, you can delete all backup data of the server to release the anti-ransomware capacity. For more information, see the "Delete backup data" section of the Create a restoration task topic.

What do I do if the status of an anti-ransomware policy is abnormal?

If the status of an anti-ransomware policy is abnormal, you cannot back up server data based on the anti-ransomware policy. We recommend that you handle the exception based on the causes that are provided on the **Anti-blackmail** page. Possible causes and solutions:

- **Insufficient anti-ransomware capacity**
  If the capacity used for data backup exceeds the capacity that you purchased, the current backup tasks are suspended and you cannot create restoration tasks. You must purchase sufficient anti-ransomware capacity to continue to use the anti-ransomware feature. For more information, see Upgrade and downgrade Security Center.
- **The Security Center agent is offline**
  If the Security Center agent is offline, the status of anti-ransomware policies is abnormal. You must handle the exception based on the causes. For more information, see Troubleshoot why the Security Center agent is offline.
- **Data backup errors**
  An invalid directory in a restoration task or insufficient server disk capacity causes data backup failures. In this case, the status of anti-ransomware policies is abnormal. You must recreate a restoration task, specify a valid backup directory, and make sure that the server disk capacity is sufficient. After the new restoration task is completed, the status of anti-ransomware policies changes to **normal**.

After I purchase the antivirus feature, can the existing features properly run?

Yes, after you purchase the antivirus feature, all existing features properly run.

Security Center provides the antivirus feature to scan for viruses, generate alerts, and perform deep cleaning against persistent viruses, such as ransomware and mining programs. The antivirus feature does not affect the existing features.

If the remaining validity period of Security Center is three years, can I purchase web tamper proofing for one year?

No, the validity period of web tamper proofing must be the same as the validity period of Security Center.

Can web tamper proofing protect files of all sizes?

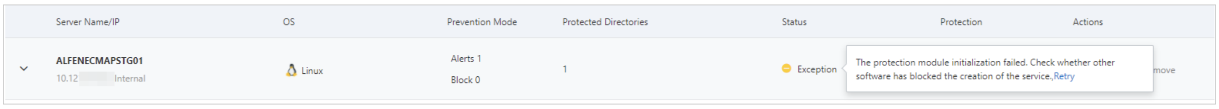
Yes, web tamper proofing can protect files of all sizes.

If my server stores more than 3 MB of files, can web tamper proofing protect the excessive files that exceed 3 MB? Can web tamper proofing protect files whose total size is not larger than 3 MB?

Yes, web tamper proofing can protect files of all sizes. Web tamper proofing can protect the files on your servers regardless of whether the total file size is larger than 3 MB.

The message "The protection module initialization failed. Check whether other software has blocked the creation of the service" appears when I enable web tamper proofing. Why?

If the web tamper proofing feature fails to be enabled and the message "The protection module initialization failed. Check whether other software has blocked the creation of the service" appears, the web tamper proofing program is blocked by third-party security software on your server.



	Server Name/IP	OS	Prevention Mode	Protected Directories	Status	Protection	Actions
⌄	ALFENECMAPSTG01 10.12[redacted] Internal	Linux	Alerts 1 Block 0	1	● Exception	The protection module initialization failed. Check whether other software has blocked the creation of the service.,Retry	move

We recommend that you add the process of the Security Center agent to the whitelists of the third-party security software on your server. You can also disable the blocking feature of the third-party security software.

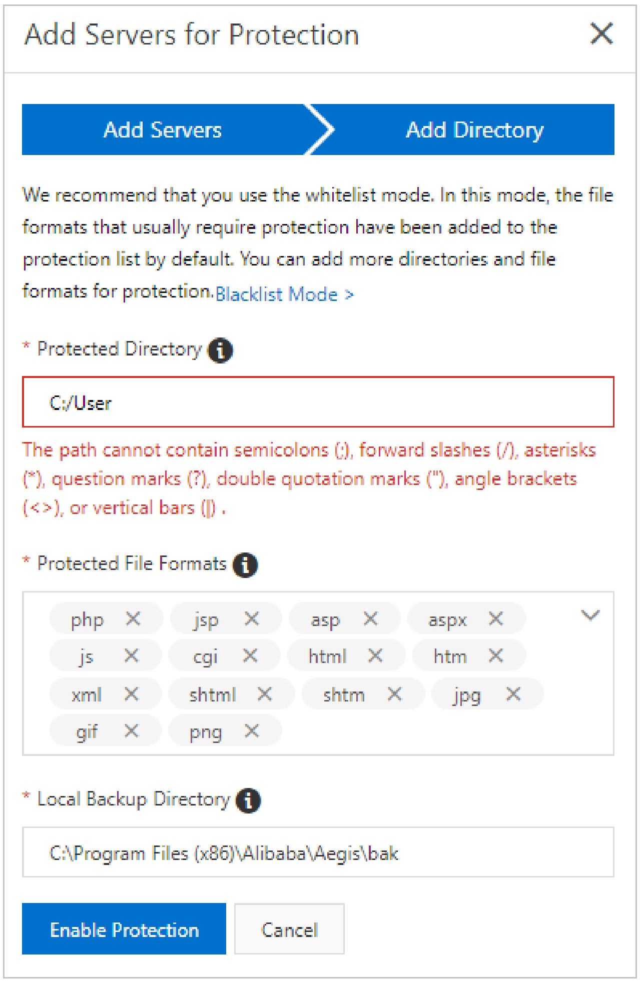
What are the requirements for the local backup directory of web tamper proofing?

The local backup directory of web tamper proofing stores the backups of a protected directory. The local backup directory can be empty. You can specify a protected directory that contains the files of your website.

If you want to protect multiple directories of a server, you can restore the backup files in different directories or in the same directory.

What do I do if I receive a message that indicates that a protected directory is invalid?

When you specify a protected directory in Windows, use a backslash (\) instead of a forward slash (/). Example: `C:\Program Files\Common Files` .



Add Servers for Protection

We recommend that you use the whitelist mode. In this mode, the file formats that usually require protection have been added to the protection list by default. You can add more directories and file formats for protection. Blacklist Mode >

* Protected Directory

C:/User

The path cannot contain semicolons (;), forward slashes (/), asterisks (*), question marks (?), double quotation marks ("), angle brackets (<>), or vertical bars (|) .

* Protected File Formats

php ✕ jsp ✕ asp ✕ aspx ✕ js ✕ cgi ✕ html ✕ htm ✕ xml ✕ shtml ✕ shtm ✕ jpg ✕ gif ✕ png ✕

* Local Backup Directory

C:\Program Files (x86)\Alibaba\Aegis\bak

Note A protected directory cannot contain the following characters: /;*?""<>|

Why does web tamper proofing remain disabled after I specify a protected directory?

After you specify a protected directory, you must turn on the switch for web tamper proofing and make sure that the Security Center agent runs as expected to enable web tamper proofing.

We recommend that you perform the following steps:

- Check whether the files that you want to protect are added to the protected directory.
- After you specify the protected directory, check whether the switch for web tamper proofing is turned on.
  You must turn on the switch for the protected directory before web tamper proofing can take effect.
- Check whether the Security Center agent runs as excepted.
  You can log on to the , choose **Defense > Tamper Protection**, and click the **Management** tab to view the status of the Security Center agent on a server. If the status is **Exception**, we recommend that you turn on the switch in the Protection column for the server again. If the status is **Offline**, we recommend that you reinstall the Security Center agent for the server. For more information, see Install the Security Center agent.

- Check whether the server has sufficient disk capacity. If the server does not have sufficient disk capacity, clean up the disk at the earliest opportunity.

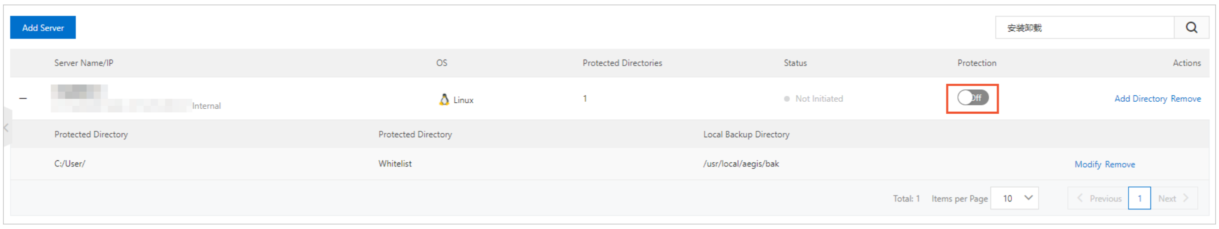
Can I write files to a protected directory on a server for which web tamper proofing is configured?

No, you cannot write files to a protected directory on a server for which web tamper proofing is configured. After you configure web tamper proofing for a server to specify a protected directory, you cannot write files to the directory.

For more information about how to write files to the protected directory, see After I enable web tamper proofing, what do I do if the website content and images cannot be modified or updated?.

After I specify a protected directory, what do I do if web tamper proofing does not immediately take effect?

After you specify a protected directory, web tamper proofing does not immediately take effect and you can still write files to the directory. To enable web tamper proofing, you must go to the **Management** tab, turn off **Protection** for the server where the directory is located, and then turn on **Protection** again.



Server Name/IP	OS	Protected Directories	Status	Protection	Actions
[redacted] Internal	Linux	1	Not Initiated	Off	Add Directory Remove

Protected Directory	Protected Directory	Local Backup Directory	
C:/User/	Whitelist	/usr/local/aegis/bak	Modify Remove

Total: 1 Items per Page 10 Previous 1 Next

I do not receive alert notifications after I log on to my server over SSH and modify the files that are protected by web tamper proofing. Why?

If you log on to your server for which web tamper proofing is enabled by using Secure Shell (SSH) and modify a file in the protected directory of the server, alerts are not generated on the **Tamper Protection** page to remind you of the modification. The following list describes the possible causes:

- **Protection** is turned off.
- You have modified the settings of the protected directory on a server for which **Protection** is turned on. After the modification, you do not turn on **Protection** again to enable web tamper proofing.
- The protected file is added to the whitelist of web tamper proofing.
  Files in the whitelist are trusted. Therefore, web tamper proofing does not block or generate alerts for modifications on the files. For more information, see Add blocked processes to a whitelist.
- The kernel version of your server is not supported by web tamper proofing.
  If an attempt is made to modify the files in the protected directory, web tamper proofing blocks the modification and does not generate alerts.

> **Note** After you modify a file in your server and save the modification, you can view that the modification was blocked by web tamper proofing in the handled alert list of the **Tamper Protection** page. You can log on to your server and view that the modification on the file does not take effect.

After I enable web tamper proofing, what do I do if the website content and images cannot be modified or updated?

You can use one of the following two methods to resolve this issue:

- Disable web tamper proofing and update the website content. After the update is complete, enable web tamper proofing. For more information about how to enable web tamper proofing, see Enable the web tamper proofing feature.
- Exclude website paths that you want to modify from the protected directory.

> ? **Note** Web tamper proofing allows you to add Linux and Windows processes to a whitelist. This ensures that protected files are updated in real time. For more information, see Add blocked processes to a whitelist.

What do I do if I receive an email or text message that notifies me of a webshell detected on my server?

If you receive an email or text message that notifies you of a webshell detected on your server, your server is attacked. A webshell file is also implanted into the server. The attacker may manipulate the data on your website or database. You can quarantine the webshell file in Security Center. We recommend that you locate and fix the vulnerability. Otherwise, the attacker may exploit the vulnerability.

My Security Center runs the Enterprise edition. Can I use the container firewall feature?

No, you cannot use the container firewall feature.

Do I need to pay for the container firewall feature?

No, you do not need to pay for the container firewall feature. After you purchase the Ultimate edition of Security Center, you can use the container firewall feature free of charge.

After I upgrade my Security Center to the Ultimate edition, does Security Center protect only containers?

No, the Ultimate edition of Security Center can protect both containers and ECS instances.