

Alibaba Cloud Threat Detection

Investigation

Issue: 20190919

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK.
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Log analysis.....	1
1.1 Limits.....	1
1.2 Activate Log Analysis Service.....	1
1.3 Log types and parameters.....	2
2 Asset fingerprints.....	7

1 Log analysis

1.1 Limits

All logs of Security Center are stored in the dedicated `sas - log` Logstore. You can find this Logstore in the `sas - log - Alibaba Cloud account ID - region ID` project.

After the log Security Center is enabled for log analysis, the system automatically creates a logstore (logstore name `sas - log`) dedicated to Security Center and stores the log data of Security Center. Please be careful not to delete it by mistake.



Notice:

If you delete the Logstore by mistake, the background will prompt "sas-log log library does not exist", and all your current log data will be lost. You need to submit a work order reset process. After the reset, you need to re-open the log analysis service before you can continue to use log analysis. Lost log data cannot be recovered.

Logstore limits

- You cannot use the Log Service API or SDK to write data into Logstores or modify the attributes of a Logstore, such as the storage period.
- To use Log Service, you must purchase and activate Log Service in Security Center first. After you purchase Log Service in Security Center, you do not have to pay additional fee in Log Service.
- The default reports may be updated later.
- The maximum storage of the Security Center Logstore is 50 TB. We recommend that you periodically back up and clear the Logstore.

1.2 Activate Log Analysis Service

Security Center Enterprise Edition supports full log service and provides features for accurate real-time log querying and log analysis.

Prerequisites

All logs of Security Center are stored in the `sas - log` Logstore. You can find the Logstore in the `sas - log - Alibaba Cloud account ID - zone` project that stores logs of the Log Service.

To use the Log Analysis Service, you need to activate and purchase the service in the Security Center console.

If you are using the Security Center Basic Edition and want to use the Log Analysis Service, you need to upgrade to the Enterprise Edition first. For more information, see [Renewal and upgrade](#).

Procedure

1. Log on to the [Security Center](#) console.
2. In the left-side navigation pane, click Investigation > Log Analysis to enter the Activate Log Analysis page.
3. Click Activate Now on the Activate Log Analysis page.
4. On the Purchase page, check Full Log and configure some other settings as needed.
5. Click Purchase Now.
6. After you confirm your order, check Security Center Agreement.
7. Click Purchase to complete the Log Analysis Service purchase.
8. In the Activate Log Analysis page, click Authorize RAM User to complete the authorization.

After the authorization is complete, you can use the Log Analysis Service in Security Center.

1.3 Log types and parameters

By default, Threat Detection Service (TDS) enables security logs, network logs, and host logs, with 14 subtypes in total to protect your assets in real time.

By default, all these three types of logs are enabled in Security Center.

- Security logs
 - Vulnerability logs
 - Baseline logs
 - Security alerting logs
- Network logs
 - DNS logs
 - Local DNS logs
 - Network session logs
 - Web logs

**Note:**

Only enterprise edition users support viewing Network logs, while advanced edition users do not. That is, advanced edition users can only view the Security logs and Server logs on the console log analysis page.

- Server logs
 - Process initiation logs
 - Network connection logs
 - System logon logs
 - Brute-force cracking logs
 - Process snapshots
 - Account snapshots
 - Port listening snapshots

Security logs

The parameters of security logs are described in the following table:

Log source	Topic (__topic__)	Description	Note
Vulnerability logs.	sas-vul-log	Vulnerability logs.	Real-time collection .
Baseline logs	sas-hc-log	Baseline logs	Real-time collection .
Security alerting logs.	sas-security-log	Security alerting logs.	Real-time collection .

Network logs

Parameters of network logs are described in the following table:

Log source	Topic (__topic__)	Description	Note
DNS logs	sas-log-dns	DNS logs of the public network.	Collection delayed for two hours.
Local DNS logs	local-dns	DNS resolution logs between ECS instances in the same Alibaba Cloud domain.	Collection delayed for one hour.
Network session log	sas-log-session	Network logs with specific protocols.	Collection delayed for one hour.
Web log	sas-log-web	HTTP logs	Collection delayed for one hour.

Server logs

The parameters of the server logs are described in the following table:

Log source	Topic (__topic__)	Description	Note
Process initiation log	aegis-log-process	Logs of process initiation on the server.	Real-time collection . When the collection process starts, it uploads reports immediately.
Network connection log	aegis-log-network	Quintuple information attached to the host .	Real-time collection on Windows. Collection on Linux with a delay of ten seconds. The information is uploaded incrementally.
System logon log	aegis-log-login	Logs of successful SSH and RDP logons.	Real-time collection .

Log source	Topic (__topic__)	Description	Note
Brute-force cracking log	aegis-log-crack	Logon failure logs.	Real-time collection .
Process snapshots	aegis-snapshot-process	Logs of process initiation on the server.	Data is not available until the feature for collecting asset fingerprints is enabled. Collects the data of each server once a day at random times.
Account snapshots	aegis-snapshot-host	Account snapshot information on the host	Data is not available until the feature for acquiring asset fingerprints is enabled. Collects the data of each server once a day at random times.
Port listening snapshots	aegis-snapshot-port	Information on port listening snapshots on the host.	Data is not available until the feature of collecting asset fingerprints is enabled. Collects the data of each server once a day at random times.

Security operation logs

Security operation logs provide the following types of logs, which are used to search for different data. _ Topic _ To distinguish:

Log source	Description	Note
Vulnerability logs.	Vulnerability logs.	Logs are generated by Security operations. Real-time collection.
Baseline logs	Baseline logs	Logs are generated by Security operations. Real-time collection.

Log source	Description	Note
Security alerting logs.	Security alerting logs.	Logs are generated by Security operations. Real-time collection.

2 Asset fingerprints

The asset fingerprint feature periodically collects the following information on your servers: processes, system accounts, listener ports, software, and website backgrounds. You can view the status of your assets and perform retrospective analysis using this information. This document describes how to view different asset fingerprints.

Function description

The asset fingerprint feature contains the following modules:

- **Processes:** Periodically collects information about processes on the server.
Scenarios: to check which server is running a specific process, and to check which processes are initiated by a specific server.
- **Accounts:** Periodically collects system account information on the server.
Scenarios: to check which server has created a specific account, and to check which accounts are created by a specific server.
- **Listener ports:** Periodically collects information about listener ports on the server.
Scenarios: to check which server is listening on a specified port, and to check which ports are enabled on a specified server.
- **Software:** Periodically collects software version information on the server.
Scenarios: to check for illegal software installations, to check for obsolete software versions, and to quickly find the affected assets when vulnerabilities are exploited.
- **Website backgrounds:** Periodically collects logon information at website backgrounds, detects weak passwords and user enumeration attempts, and monitors background security. Scenarios: to view logon records at backgrounds, to check whether weak passwords exist, and to view user enumeration attempts.

Additionally, for information about processes, system accounts, listener ports, and software, you can specify the frequency of data collection.

View asset fingerprints for an individual asset

You can access the asset details of a specific asset through the Assets page and view the asset fingerprints of this asset. The individual asset fingerprints include processes, accounts, listener ports, and software.

1. Log on to the [Security Center console](#).

2. Go to the Assets page, select the asset you want to view, and click its Asset IP/Name.

3. On the asset details page, click Asset Fingerprints.

- View processes

a. Go to the Processes page to view all the running processes on the asset. You can search by process name or user.

b. Set Data Type to Historical to view the process changes, including New Process and Stopped Process.

Basic Information Vulnerabilities 5 Baseline Risks 2 Events 113 Asset Fingerprints Security Configuration

Listener Ports Processes Accounts Software

Search: Process Username Search Reset Last Updated At : 2018-07-19 11:44:38 Refresh

Data Type: Latest Historical

Status: New Process Stopped Process

Status	Process	Process Path	Required Parameter	Start At	Username	Permission	PID	Parent Process	File MD5	Status Changed At
Start	sshd	/usr/bin/sshd		2018-07-05 20:51:41	root		30517	systemd	N/A	2018-07-19 11:44:38
Start	irqbalance	/usr/sbin/irqbalance --foreground		2018-07-04 11:56:32	root		475	systemd	15cbccb202bc37a80831ed97301cbbb2	2018-07-19 11:44:38

c. Click a process name to view the details.

- View accounts

a. Go to the Accounts page to view all the logged-on system accounts on the asset. You can search by account name.

b. Set Data Type to Historical to view the system account changes, including New, Modified, and Deleted.

Basic Information Vulnerabilities 5 Baseline Risks 2 Events 113 Asset Fingerprints Security Configuration

Listener Ports Processes Accounts Software

Search: Username Search Reset Last Updated At : 2018-07-18 18:12:21 Refresh

Data Type: Latest Historical

Root Permissions: Yes No

Status: New Deleted Modified

Status	Username	Root Permissions	User Group	Expire At	Last Logon	Status Changed At
Create	shutdown	No	root	never	Time : -- Source : --	2018-07-18 18:12:21
Create	dbus	No	dbus	never	Time : -- Source : --	2018-07-18 18:12:21

c. Click an account name to view account details.

- View listener ports
 - a. Go to the Listener Ports page to view all the enabled ports and the network protocols on the asset. You can search by port number or process name.
 - b. Set Data Type to Historical to view the listener port changes, including New Listener and Disabled Listener.

Status	Port	Protocol	Process	Listener IP	Updated At
Stop	80	tcp	nginx	0.0.0.0	2018-07-19 16:20:09
Start	999	tcp	ncat	0.0.0.0	2018-07-18 17:38:55
Start	80	tcp	nginx	0.0.0.0	2018-07-18 17:38:55

- c. Click a port number to view the details.
- View software
 - a. Go to the Software page to view all the software on the asset. You can search by process, version, or installation directory.
 - b. Set Data Type to Historical to view the software changes, including Install, Uninstall, and Update Version.

Status	Process	Software	Last Updated At	Software Installation Path	Status Changed At
Install	pyxdtr	0.5.1	2017-10-15 23:19:21	/usr/lib64/python2.7/site-packages/pyxdtr-0.5.1-py2.7.egg-info	2018-07-19 16:45:35
Install	fipscheck	1.4.1	2017-10-15 23:19:24	/usr/bin/fipscheck	2018-07-19 16:45:35

- c. Click a software name to view the details.

View asset fingerprints for all assets

You can view the asset fingerprints for all assets on the Asset Fingerprints page. The Asset Fingerprints page displays the real-time information for processes, accounts, listener ports, software, and website backgrounds.

Follow these steps to view asset fingerprints for all assets:

1. Log on to the [Security Center console](#).
2. In the left-side navigation pane, click More.

3. Click Asset Fingerprints.

- View processes

a. Go to the Processes page to view all the processes and servers that are running them. You can search by process name or user.

b. Click a process name to view the details.

Process: sshd [Back](#)

Search: All Assets [Search by server IP or name](#) [Search by server tag](#) [Search](#) [Reset](#)

Asset	Process Path	Required Parameter	Start At	Username	Permission	PID	Parent Process	File MD5	Updated At
10.10.10.10	/usr/bin/sshd	/usr/bin/sshd	2018-07-17 17:08:02	root	root	2299	systemd	N/A	2018-07-19 11:44:29
10.10.10.10	/usr/bin/sshd	/usr/bin/sshd	2018-07-04 14:08:29	root	root	9845	systemd	N/A	2018-07-19 11:44:29

- View system accounts

a. Go to the System Accounts page to view all the logged-on accounts and servers that are using them. You can search by account name.

b. Click an account name to view account details.

Account: root [Back](#)

Search: All Assets [Search by server IP or name](#) [Search by server tag](#) [Search](#) [Reset](#)

Root Permissions: [Yes](#) [No](#)

Asset	Root Permissions:	User Group	Expire At	Last Logon	Updated At
10.10.10.10	Yes	root	never	Time : 2018-07-18 17:43:59 Source : 106.11.34.17	2018-07-18 18:12:21
10.10.10.10	Yes	root	never	Time : 2018-07-04 11:49:25 Source : 47.254.216.188	2018-07-18 18:12:21

- View listener ports

a. Go to the Listener Ports page to view all the enabled ports, protocols, and servers that are using them. You can search by port number or process name.

b. Click a port number to view the details.

Port: 22 [Back](#)

Search: All Assets [Search by server IP or name](#) [Search by server tag](#) [Process](#) [Search](#) [Reset](#)

Servers	Process	Asset	Updated At
10.10.10.10 [redacted]	sshd	0.0.0.0	2018-07-18 18:12:22
10.10.10.10 [redacted]	sshd	0.0.0.0	2018-07-19 16:44:41

- View software

- Go to the Software page to view all the software and servers that are using them. You can search by process, version, or by installation directory.
- Click a software name to view the details.

Software: rsyslog [Back](#)

Search: All Assets [Search by server IP or name](#) [Search by server tag](#) [Software](#) [Software Installation Path](#) [Search](#) [Reset](#)

Asset	Software	Last Updated At	Software Installation Path	Updated At
10.10.10.10 [redacted]	8.24.0	2017-10-15 23:19:42	/etc/logrotate.d/syslog	2018-07-18 18:12:45
10.10.10.10 [redacted]	8.24.0	2017-10-15 23:19:42	/etc/logrotate.d/syslog	2018-07-19 16:44:47

- View website background logon records: Go to the Website Background page to view the background logon records, weak logon passwords, and user enumerations attempts.

Asset Fingerprints [Back](#) [Settings](#)

Processes System Accounts Listener Ports Software Website Background

Name	Background Address	Weak Password	Yesterday User Enumerations	Previous User Enumerations	Last Detected At	First Detected At
<p> Could not find any record that met the condition.</p>						

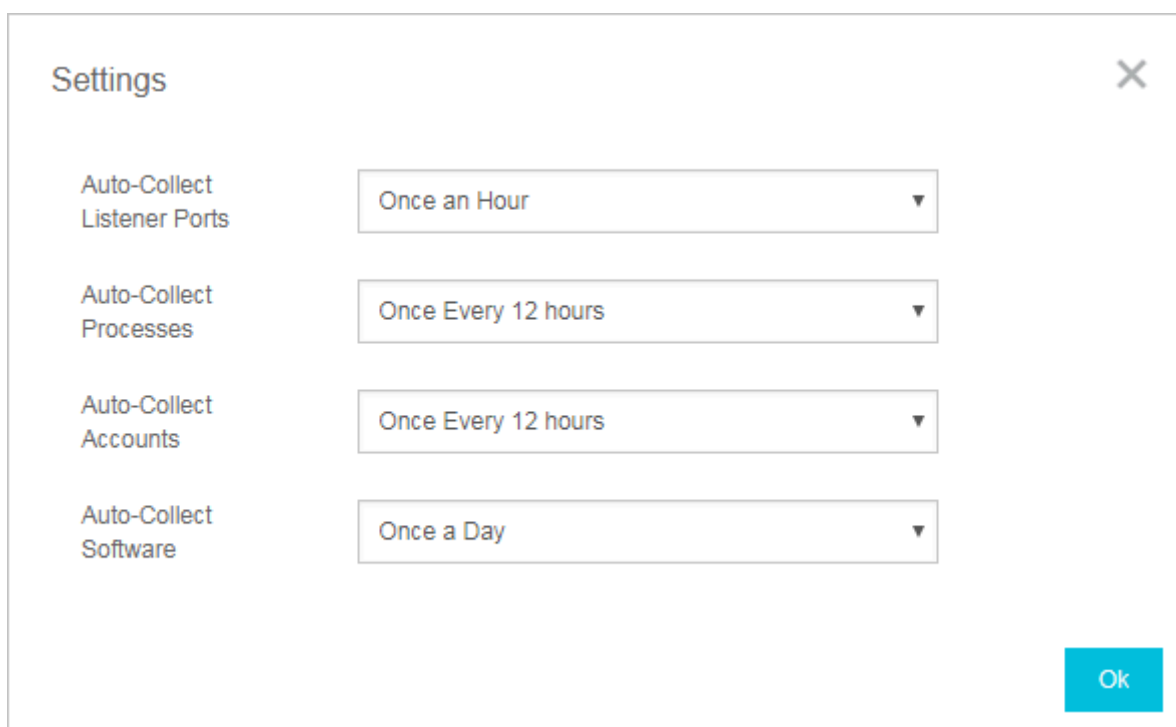
Settings

On the Asset Fingerprints Settings page, you can specify the frequency of data collection for processes, system accounts, listener ports, and software.

You can specify the frequency of data collection by following these steps:

- Log on to the [Security Center console](#).
- In the left-side navigation pane, click More.

3. Click Asset Fingerprints.
4. In the upper right corner of the page, click Settings.
5. Complete the following settings:



The screenshot shows a 'Settings' dialog box with a close button (X) in the top right corner. It contains four settings, each with a label and a dropdown menu:

Setting	Value
Auto-Collect Listener Ports	Once an Hour
Auto-Collect Processes	Once Every 12 hours
Auto-Collect Accounts	Once Every 12 hours
Auto-Collect Software	Once a Day

An 'Ok' button is located in the bottom right corner of the dialog box.

- Select Auto-Collect Listener Ports and choose from the following: Disabled, Once an Hour, Once Every 3 Hours, Once Every 12 Hours, Once a Day, or Once a Week.
 - Select Auto-Collect Processes and choose from the following: Disabled, Once an Hour, Once Every 3 Hours, Once Every 12 Hours, Once a Day, or Once a Week.
 - Select Auto-Collect System Accounts and choose from the following: Disabled, Once an Hour, Once Every 3 Hours, Once Every 12 Hours, Once a Day, or Once a Week.
 - Select Auto-Collect Software and choose from the following: Disabled, Once an Hour, Once Every 3 Hours, Once Every 12 Hours, Once a Day, or Once a Week.
6. Click OK to apply the settings.