ALIBABA CLOUD

Alibaba Cloud

Security Center

Investigation

Document Version: 20220616

Alibaba Cloud

Legal disclaimer

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

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

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

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

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

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

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

Document conventions

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

Table of Contents

1.Log analysis

1.1. Overview

Full logs of Security Center are stored in a dedicated Logstore. You can find the Logstore in the project that stores Security Center logs in the Log Service console. The name of the project is in the sas-log-ID of your Alibaba Cloud account-Region ID format.

After you enable log analysis of Security Center, the system automatically creates a Logstore named *sas-log* that is dedicated to Security Center in the Log Service console. The log data of Security Center is stored in the newly created Logstore. We recommend that you do not delete this Logstore.

> **Notice** If you delete the Logstore by mistake, a message appears, indicating that **the sas-log Logstore does not exist** and all the log data in your current Logstore is lost. In this case, you must to undo the operation. After you undo the operation, you must enable log analysis again to use the feature. You cannot recover lost log data.

Logstore limits

- You cannot use the Log Service API or SDKs to import data into a Logstore or modify the attributes of the Logstore, such as the retention period.
- To enable log analysis of Security Center, you must activate Log Service and purchase log storage capacity.
- The default reports may be updated in later versions.
-

Regions for log storage

After you enable log analysis, Security Center automatically creates three projects that store the log data of Security Center.

The following table describes the source regions of log data to be stored in these projects.

Region of the project	Source region of log data
China (Hangzhou)	Regions in mainland China
Singapore (Singapore)	Regions outside China
Malaysia (Kuala Lumpur)	N/A

1.2. Enable log analysis

Security Center provides the log analysis feature that allows you to query and analyze logs in real time. This topic describes how to enable log analysis.

Context

You must enable log analysis in the Security Center console before you can use log analysis.

Before you use the feature, make sure that you use the , , , or edition and have purchased log storage capacity. If you use the edition, you must upgrade Security Center to the , , , or edition and purchase log storage capacity before you can use the feature. For more information about how to purchase and upgrade Security Center, see Purchase Security Center and Upgrade and downgrade Security Center. For more information about the features that each edition supports, see Features.

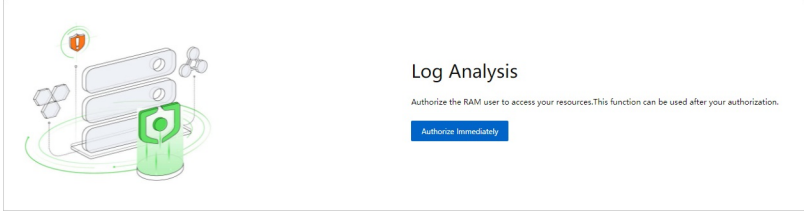
> **Notice** By default, the following logs are enabled in Security Center: security logs, network logs, and host logs.

After you enable log analysis in the Security Center console, Log Service automatically creates a dedicated Logstore to store Security Center logs. You can view information about the Logstore in the . For more information about Logstore limits, see Limits.

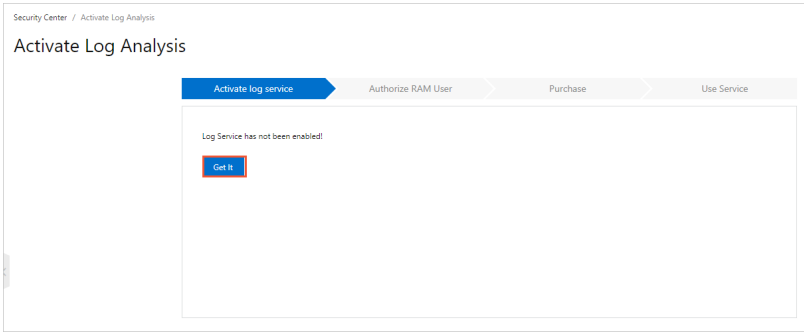
> **Note** The log analysis feature is a value-added feature that requires additional service fees. The storage fee for 1 TB of logs is USD 72.9 per month. As required by the Cyber Security Law, logs are retained for at least 180 days. We recommend that you allocate the log storage capacity of 40 GB to each server to store logs.

Procedure

1.
2.
3. If you have not authorized Security Center to access your cloud resources, click **Authorize Immediately**.

   Security Center must be authorized to access your cloud resources. After Security Center is authorized, Resource Access Management (RAM) automatically creates a RAM role named **AliyunServiceRoleForSas**. Security Center uses this RAM role to access cloud resources of your services and protect the resources. For more information,see Service-linked roles.
4. In the **Activate Log Analysis** wizard, click **Activate now**.

5. In the **Purchase** step, click **Activate now**.
6. On the buy page of Security Center, configure the Edition and **Log Analysis** parameters.

You must select the , , or edition. As required by the Cyber Security Law, logs are retained for at least 180 days. We recommend that you allocate the log storage capacity of 40 GB to each server to store logs.

7. Click **Buy Now**.
8. Read and select **Security Center Agreement of Service** and click **Pay**.
9. Return to the **Log Analysis** page and click **Log Analysis has been activated.**

   After you enable log analysis, you can use it to query and analyze logs.

1.3. Log types and parameters

By default, Security Center collects security logs, network logs, and host logs based on the log analysis feature to protect your assets in real time.

By default, Security Center collects the following types of logs:

- **Security logs**
  - Vulnerability logs
  - Baseline logs
  - Alert logs
- **Network logs**
  - Domain Name System (DNS) logs
  - Internal DNS logs
  - Network session logs
  - Web access logs

  > Note
- **Host logs**
  - Process startup logs
  - Network connection logs
  - Logon logs
  - Brute-force attack logs
  - Process snapshots
  - Account snapshots
  - Port snapshots

Security logs

The following table describes the parameters of security logs.

Log type	Topic (__topic__)	Description	Collection cycle
Vulnerability logs	sas-vul-log	Vulnerability-related logs	Logs are collected in real time.
Baseline logs	sas-hc-log	Baseline risk-related logs	Logs are collected in real time.
Alert logs	sas-security-log	Alert logs	Logs are collected in real time.

Network logs

The following table describes the parameters of network logs.

Log type	Topic (__topic__)	Description	Collection cycle
DNS logs	sas-log-dns	DNS logs of the Internet	Logs are collected 2 hours after the logs are generated.
Internal DNS logs	local-dns	DNS logs between Elastic Compute Service (ECS) instances in the same Alibaba Cloud domain	Logs are collected 1 hour after the logs are generated.
Network session logs	sas-log-session	Network logs of specific protocols	Logs are collected 1 hour after the logs are generated.
Web access logs	sas-log-http	HTTP traffic logs generated when a server communicates with the Internet	Logs are collected 1 hour after the logs are generated.

Host logs

The following table describes the parameters of host logs.

Log type	Topic (__topic__)	Description	Collection cycle
Process startup logs	aegis-log-process	Logs related to the startup of server processes	Logs are collected in real time. When a process starts, it is immediately reported.

Log type	Topic (__topic__)	Description	Collection cycle
Network connection logs	aegis-log-network	Logs related to the 5-tuples that are connected to servers	• Windows operating systems: Logs are collected in real time. • Linux operating systems: Logs are collected every 10 seconds. Incremental logs are reported.
Logon logs	aegis-log-login	Logs of successful SSH and RDP logons	Logs are collected in real time.
Brute-force attack logs	aegis-log-crack	Logs related to logon failures	Logs are collected in real time.
Process snapshots	aegis-snapshot-process	Information about the snapshots of processes on servers	Data is available only after asset fingerprint collection is enabled. The data of each server is collected once a day at random times.
Account snapshots	aegis-snapshot-host	Information about the snapshots of accounts on servers	Data is available only after asset fingerprint collection is enabled. The data of each server is collected once a day at random times.
Port snapshots	aegis-snapshot-port	Information about the snapshots of port listening on servers	Data is available only after asset fingerprint collection is enabled. The data of each server is collected once a day at random times.

1.4. Log fields

This topic describes the log fields of Security Center.

Real-time logs

Field name	Description	Example
dir	The direction of the network connection. Valid values: • in: inbound • out: outbound	in

Field name	Description	Example
src_ip	The source IP address. • If the value of dir is out, the value of this field is the IP address of your host. • If the value of dir is in, the value of this field is the IP address of the peer host.	10.240.XX.XX
src_port	The source port.	24680
dst_ip	The destination IP address. • If the value of dir is out, the value of this field is the IP address of the peer host. • If the value of dir is in, the value of this field is the IP address of your host.	10.240.XX.XX
dst_port	The destination port.	22
status	The status of the network connection. **Note** In real-time logs, the value of this field is random. You can ignore this field.	2
type	The type of the real-time network connection. Valid values: • connect: TCP connection initiated • accept: TCP connection received • listen: port listening	listen

Snapshot logs (asset fingerprints)

Field name	Description	Example
proc_path	The path of the process.	"/usr/sbin/sshd"
proc_cmdline	The command line of the process.	"/usr/sbin/sshd -D"
pid	The ID of the process.	1158

Field name	Description	Example
ppid	The ID of the parent process.	1
dir	The direction of the network connection. Valid values: • in: inbound • out: outbound	in
src_ip	The source IP address. • If the value of dir is out, the value of this field is the IP address of your host. • If the value of dir is in, the value of this field is the IP address of the peer host.	10.240.XX.XX
src_port	The source port.	24680
dst_ip	The destination IP address. • If the value of dir is out, the value of this field is the IP address of the peer host. • If the value of dir is in, the value of this field is the IP address of your host.	10.240.XX.XX
dst_port	The destination port.	22
status	The status of the network connection. Valid values: • 1: TCP_STATE_CLOSED • 2: TCP_STATE_LISTEN • 3: TCP_STATE_SYN_SENT • 4: TCP_STATE_SYN_RCVD • 5: TCP_STATE_ESTABLISHED • 6: TCP_STATE_CLOSE_WAIT • 7: TCP_STATE_CLOSING • 8: TCP_STATE_FIN_WAIT1 • 9: TCP_STATE_FIN_WAIT2 • 10: TCP_STATE_LAST_ACK • 11: TCP_STATE_TIME_WAIT	2

Network logs

Domain Name System (DNS) logs

Field name	Description	Example
additional	The additional field. Multiple additional fields are separated by vertical bars (|).	None
additional_num	The number of additional fields.	0
answer	The DNS answer. Multiple DNS answers are separated by vertical bars (|).	example.com A IN 52 1.2.XX.XX
answer_num	The number of DNS answers.	1
authority	The authority field.	NS IN 17597
authority_num	The number of authority fields.	1
client_subnet	The subnet of the client.	172.168.XX.XX
dst_ip	The destination IP address.	1.2.XX.XX
dst_port	The destination port.	53
in_out	The direction of data transmission. Valid values: • **in**: inbound • **out**: outbound	out
qid	The ID of the query.	12345
qname	The domain name that is queried.	example.com
qtype	The type of the query.	A
query_datetime	The timestamp of the query. Unit: milliseconds.	1537840756263
rcode	The code returned.	0
region	The ID of the source region. Valid values: • 1: China (Beijing) • 2: China (Qingdao) • 3: China (Hangzhou) • 4: China (Shanghai) • 5: China (Shenzhen) • 6: other regions	1
response_datetime	The response time.	2018-09-25 09:59:16

Field name	Description	Example
src_ip	The source IP address.	1.2.XX.XX
src_port	The source port.	22

Internal DNS logs

Field name	Description	Example
answer_rda	The DNS answer. Multiple DNS answers are separated by vertical bars (|).	example.com
answer_ttl	The time to live (TTL) of the DNS answer. Multiple TTLs are separated by vertical bars (|).	100
answer_type	The type of the DNS answer. Multiple types are separated by vertical bars (|).	1
anwser_name	The name of the DNS answer. Multiple names are separated by vertical bars (|).	example.com
dest_ip	The destination IP address.	1.2.XX.XX
dest_port	The destination port.	53
group_id	The ID of the group.	3
hostname	The name of the host.	hostNmae
id	The ID of the query.	64588
instance_id	The ID of the instance.	i-2zeg4zldn8zypsfg****
internet_ip	The public IP address.	1.2.XX.XX
ip_ttl	The TTL of the IP address.	64
query_name	The domain name that is queried.	example.com
query_type	The type of the query.	A
src_ip	The source IP address.	1.2.XX.XX
src_port	The source port.	1234
time	The timestamp of the query. Unit: seconds.	1537840756

Field name	Description	Example
time_usecond	The response duration. Unit: microseconds.	49069
tunnel_id	The ID of the tunnel.	514763

Network session logs

Field name	Description	Example
asset_type	The type of the asset from which the logs are collected. Valid values: • ECS • SLB • RDS	ECS
dst_ip	The destination IP address.	1.2.XX.XX
dst_port	The destination port.	53
proto	The protocol type. Valid values: • tcp • udp	tcp
session_time	The time when the session starts.	2018-09-25 09:59:49
src_ip	The source IP address.	1.2.XX.XX
src_port	The source port.	54

Web access logs

Field name	Description	Example
content_length	The length of the message body. Unit: bytes.	123
dst_ip	The destination IP address.	1.2.XX.XX
dst_port	The destination port.	54
host	The host that is accessed.	47.XX.XX.158:8080
jump_location	The redirection address.	123
method	The HTTP request method.	GET

Field name	Description	Example
referer	The HTTP referer. The field contains the URL of the web page that is linked to the resource being requested.	www.example.com
request_datetime	The time when the request is initiated.	2018-09-25 09:58:37
ret_code	The HTTP status code returned.	200
rqs_content_type	The type of the request content.	text/plain;charset=utf-8
rsp_content_type	The type of the response content.	text/plain; charset=utf-8
src_ip	The source IP address.	1.2.XX.XX
src_port	The source port.	54
uri	The request URI.	/report
user_agent	The user agent that initiates the request.	okhttp/3.2.0
x_forward_for	The routing information.	1.2.XX.XX

Security logs

Vulnerability logs

Field name	Description	Example
name	The name of the vulnerability.	oval:com.redhat.rhsa:def:20182390
alias_name	The alias of the vulnerability.	RHSA-2018:2390: kernel security and bug fix update
op	The operation on the vulnerability. Valid values: • new • verify • fix	new
status	The status of the vulnerability.	1

Field name	Description	Example
tag	The tag of the vulnerability. Valid values: • oval: Linux software vulnerability • system: Windows system vulnerability • cms: Web-CMS vulnerability **Note** A random string indicates other types of vulnerabilities.	oval
type	The type of the vulnerability. Valid values: • sys: Windows system vulnerability • cve: Linux software vulnerability • cms: Web-CMS vulnerability • emg: urgent vulnerability	sys
uuid	The UUID of the server.	1234-b7ca-4a0a-9267-12****

Baseline logs

Field name	Description	Example
level	The severity of the risk item. Valid values: • high • medium • low	low
op	The operation. Valid values: • new • verity: verification	new
risk_name	The name of the risk item.	Password compliance checks
status	The information about the status. For more information, see Status codes of security logs.	1

Field name	Description	Example
sub_type_alias	The alias of the sub type in Chinese.	System account security
sub_type_name	The name of the sub type.	system_account_security
type_name	The name of the check type.	account
type_alias	The alias of the type in Chinese.	cis
uuid	The UUID of the server on which risk items are detected.	12345-b7ca-4a0a-9267-123456

Baseline types and sub types

Type	Sub type	Description
hc_exploit	hc_exploit_redis	High risk exploit-Redis unauthorized access high exploit vulnerability risk
hc_exploit	hc_exploit_activemq	High risk exploit-ActiveMQ unauthorized access high exploit vulnerability risk
hc_exploit	hc_exploit_couchdb	High risk exploit - CouchDB unauthorized access high exploit risk
hc_exploit	hc_exploit_docker	High risk exploit - Docker unauthorized access high vulnerability risk
hc_exploit	hc_exploit_es	High risk exploit - Elasticsearch unauthorized access high exploit vulnerability risk
hc_exploit	hc_exploit_hadoop	High risk exploit - Hadoop unauthorized access high exploit vulnerability risk
hc_exploit	hc_exploit_jboss	High risk exploit - Jboss unauthorized access high exploit vulnerability risk
hc_exploit	hc_exploit_jenkins	High risk exploit - Jenkins unauthorized access high exploit vulnerability risk
hc_exploit	hc_exploit_k8s_api	High risk exploit - Kubernetes Apiserver unauthorized access high exploit vulnerability risk
hc_exploit	hc_exploit_ldap	High risk exploit - LDAP unauthorized access high exploit vulnerability risk (Windows)
hc_exploit	hc_exploit_ldap_linux	High risk exploit-OpenLDAP unauthorized access vulnerability baseline (Linux)
hc_exploit	hc_exploit_memcache	High risk exploit - Memcached unauthorized access high exploit vulnerability risk

Type	Sub type	Description
hc_exploit	hc_exploit_mongo	High risk exploit - Mongodb unauthorized access high exploit vulnerability risk
hc_exploit	hc_exploit_pgsql	High risk exploit-Postgresql unauthorized access to high-risk risk baseline
hc_exploit	hc_exploit_rabbitmq	High risk exploit-RabbitMQ unauthorized access high exploit vulnerability risk
hc_exploit	hc_exploit_rsync	High risk exploit - rsync unauthorized access high exploit vulnerability risk
hc_exploit	hc_exploit_tomcat	
hc_exploit	hc_exploit_zookeeper	High risk exploit - ZooKeeper unauthorized access high exploit vulnerability risk
hc_container	hc_docker	Alibaba Cloud Standard -DockerSecurity Baseline Check
hc_container	hc_middleware_ack_master	CIS standard-Kubernetes(ACK) Master node security inspection inspection
hc_container	hc_middleware_ack_node	CIS standard-Kubernetes(ACK) node security inspection
hc_container	hc_middleware_k8s	Alibaba Cloud Standard-Kubernetes-Master security baseline check
hc_container	hc_middleware_k8s_node	Alibaba Cloud Standard-Kubernetes-Node security baseline check
cis	hc_suse 15_djbh	SUSE Linux 15 Baseline for China classified protection of cybersecurity-Level III
cis	hc_aliyun_linux3_djbh_l3	Alibaba Cloud Linux 3 Baseline for China classified protection of cybersecurity-Level III
cis	hc_aliyun_linux_djbh_l3	Alibaba Cloud Linux/Aliyun Linux 2 Baseline for China classified protection of cybersecurity-Level III
cis	hc_bind_djbh	China's Level 3 Protection of Cybersecurity - Bind Compliance Baseline Check
cis	hc_centos 6_djbh_l3	CentOS Linux 6 Baseline for China classified protection of cybersecurity-Level III
cis	hc_centos 7_djbh_l3	CentOS Linux 7 Baseline for China classified protection of cybersecurity-Level III
cis	hc_centos 8_djbh_l3	CentOS Linux 8 Baseline for China classified protection of cybersecurity - Level III

Type	Sub type	Description
cis	hc_debian_djbh_l3	Debian Linux 8/9/10 Baseline for China classified protection of cybersecurity-Level III
cis	hc_iis_djbh	IIS Baseline for China classified protection of cybersecurity-Level III
cis	hc_informix_djbh	China's Level 3 Protection of Cybersecurity - Informix Compliance Baseline Check
cis	hc_jboss_djbh	Jboss6/7 Compliance Baseline Check
cis	hc_mongo_djbh	MongoDB Baseline for China classified protection of cybersecurity-Level III
cis	hc_mssql_djbh	China's Level 3 Protection of Cybersecurity -SQL Server Compliance Baseline Check
cis	hc_mysql_djbh	Equal Guarantee Level 3-MySql Compliance Baseline Check
cis	hc_nginx_djbh	Equal Guarantee Level 3-Nginx Compliance Baseline Check
cis	hc_oracle_djbh	China's Level 3 Protection of Cybersecurity - Oracle Compliance Baseline Check
cis	hc_pgsql_djbh	Level 3-PostgreSql compliance baseline check
cis	hc_redhat 6_djbh_l3	China's Level 3 Protection of Cybersecurity - Red Hat Enterprise Linux 6 Compliance Baseline Check
cis	hc_redhat_djbh_l3	China's Level 3 Protection of Cybersecurity - Red Hat Enterprise Linux 7 Compliance Baseline Check
cis	hc_redis_djbh	Redis Baseline for China classified protection of cybersecurity-Level III
cis	hc_suse 10_djbh_l3	SUSE Linux 10 Baseline for China classified protection of cybersecurity-Level III
cis	hc_suse 12_djbh_l3	SUSE Linux 12 Baseline for China classified protection of cybersecurity-Level III
cis	hc_suse_djbh_l3	SUSE Linux 11 Baseline for China classified protection of cybersecurity-Level III
cis	hc_ubuntu 14_djbh_l3	Ubuntu 14 Baseline for China classified protection of cybersecurity-Level III
cis	hc_ubuntu_djbh_l3	Waiting for Level 3-Ubuntu 16/18/20 compliance regulations inspection

Type	Sub type	Description
cis	hc_was_djbh	China's Level 3 Protection of Cybersecurity - Websphere Application Server Compliance Baseline Check
cis	hc_weblogic_djbh	Weblogic Baseline for China classified protection of cybersecurity-Level III
cis	hc_win 2008_djbh_l3	China's Level 3 Protection of Cybersecurity - Windows Server 2008 R2 Compliance Baseline Check
cis	hc_win 2012_djbh_l3	Windows 2012 R2 Baseline for China classified protection of cybersecurity-Level III
cis	hc_win 2016_djbh_l3	Windows 2016/2019 Baseline for China classified protection of cybersecurity-Level III
cis	hc_aliyun_linux_djbh_l2	Alibaba Cloud Linux/Aliyun Linux 2 Baseline for China classified protection of cybersecurity-Level II
cis	hc_centos 6_djbh_l2	CentOS Linux 6 Baseline for China classified protection of cybersecurity-Level II
cis	hc_centos 7_djbh_l2	CentOS Linux 7 Baseline for China classified protection of cybersecurity-Level II
cis	hc_debian_djbh_l2	Debian Linux 8 Baseline for China classified protection of cybersecurity-Level II
cis	hc_redhat 7_djbh_l2	Redhat Linux 7 Baseline for China classified protection of cybersecurity-Level II
cis	hc_ubuntu_djbh_l2	Linux Ubuntu 16/18 Baseline for China classified protection of cybersecurity-Level II
cis	hc_win 2008_djbh_l2	Windows 2008 R2 Baseline for China classified protection of cybersecurity-Level II
cis	hc_win 2012_djbh_l2	Windows 2012 R2 Baseline for China classified protection of cybersecurity-Level II
cis	hc_win 2016_djbh_l2	Windows 2016/2019 Baseline for China classified protection of cybersecurity-Level II
cis	hc_aliyun_linux_cis	Alibaba Cloud Linux/Aliyun Linux 2 CIS Benchmark
cis	hc_centos 6_cis_rules	CIS CentOS Linux 6 LTS Benchmark
cis	hc_centos 7_cis_rules	CIS CentOS Linux 7 LTS Benchmark
cis	hc_centos 8_cis_rules	CIS CentOS Linux 8 LTS Benchmark
cis	hc_debian 8_cis_rules	CIS Debian Linux 8 Benchmark

Type	Sub type	Description
cis	hc_ubuntu 14_cis_rules	CIS Ubuntu Linux 14 LTS Benchmark
cis	hc_ubuntu 16_cis_rules	CIS Ubuntu Linux 16/18/20 LTS Benchmark
cis	hc_win 2008_cis_rules	CIS Microsoft Windows Server 2008 R2 Benchmark
cis	hc_win 2012_cis_rules	CIS Microsoft Windows Server 2012 R2 Benchmark
cis	hc_win 2016_cis_rules	CIS Microsoft Windows Server 2016/2019 R2 Benchmark
cis	hc_kylin_djbh_l3	China's Level 3 Protection of Cybersecurity - Kylin Compliance Baseline Check
cis	hc_uos_djbh_l3	China's Level 3 Protection of Cybersecurity - uos Compliance Baseline Check
hc_best_secruity	hc_aliyun_linux	Alibaba Cloud Linux/Aliyun Linux 2 Benchmark
hc_best_secruity	hc_centos 6	Alibaba Cloud Standard - CentOS Linux 6 Security Baseline Check
hc_best_secruity	hc_centos 7	Alibaba Cloud Standard - CentOS Linux 7/8 Security Baseline Check
hc_best_secruity	hc_debian	Alibaba Cloud Standard - Debian Linux 8/9/10 Security Baseline
hc_best_secruity	hc_redhat 6	Alibaba Cloud Standard - Red Hat Enterprise Linux 6 Security Baseline Check
hc_best_secruity	hc_redhat 7	Alibaba Cloud Standard - Red Hat Enterprise Linux 7/8 Security Baseline Check
hc_best_secruity	hc_ubuntu	Alibaba Cloud Standard - Ubuntu Security Baseline
hc_best_secruity	hc_windows_2008	Alibaba Cloud Standard - Windows Server 2008 R2 Security Baseline Check
hc_best_secruity	hc_windows_2012	Alibaba Cloud Standard - Windows 2012 R2 Security Baseline
hc_best_secruity	hc_windows_2016	Alibaba Cloud Standard - Windows 2016/2019 Security Baseline
hc_best_secruity	hc_db_mssql	Alibaba Cloud Standard-SQL Server Security Baseline Check
hc_best_secruity	hc_memcached_ali	Alibaba Cloud Standard - Memcached Security Baseline Check

Type	Sub type	Description
hc_best_security	hc_mongodb	Alibaba Cloud Standard - MongoDB version 3.x Security Baseline Check
hc_best_security	hc_mysql_ali	Alibaba Cloud Standard - Mysql Security Baseline Check
hc_best_security	hc_oracle	Alibaba Cloud Standard - Oracle 11g Security Baseline Check
hc_best_security	hc_pgsql_ali	Alibaba Cloud Standard-PostgreSql Security Initialization Check
hc_best_security	hc_redis_ali	Alibaba Cloud Standard - Redis Security Baseline Check
hc_best_security	hc_apache	Alibaba Cloud Standard - Apache Security Baseline Check
hc_best_security	hc_iis_8	Alibaba Cloud Standard - IIS 8 Security Baseline Check
hc_best_security	hc_nginx_linux	Alibaba Cloud Standard - Nginx Security Baseline Check
hc_best_security	hc_suse 15	Alibaba Cloud Standard - SUSE Linux 15 Security Baseline Check
hc_best_security	tomcat 7	Alibaba Cloud Standard-Apache Tomcat Security Baseline
weak_password	hc_mongodb_pwd	Weak Password-MongoDB Weak Password baseline(support version 2. X)
weak_password	hc_weakpwd_ftp_linux	Weak password - Ftp login weak password baseline
weak_password	hc_weakpwd_linux_sys	Weak password - Linux system login weak password baseline
weak_password	hc_weakpwd_mongodb 3	Weak Password-MongoDB Weak Password baseline
weak_password	hc_weakpwd_mssql	Weak password - SQL Server DB login weak password baseline
weak_password	hc_weakpwd_mysql_linux	Weak password - Mysql DB login weak password baseline
weak_password	hc_weakpwd_mysql_win	Weak password - Mysql DB login weak password baseline(Windows version)

Type	Sub type	Description
weak_password	hc_weakpwd_openldap	Weak password - Openldap login weak password baseline
weak_password	hc_weakpwd_oracle	Weak Password-Oracle login weak password detection
weak_password	hc_weakpwd_pgsql	Weak password - PostgreSQL DB login weak password baseline
weak_password	hc_weakpwd_pptp	Weak password - pptpd login weak password baseline
weak_password	hc_weakpwd_redis_linux	Weak password - Redis DB login weak password baseline
weak_password	hc_weakpwd_rsync	Weak password - rsync login weak password baseline
weak_password	hc_weakpwd_svn	Weak password - svn login weak password baseline
weak_password	hc_weakpwd_tomcat_linux	Weak password - Apache Tomcat Console weak password baseline
weak_password	hc_weakpwd_vnc	Weak password-VncServer weak password check
weak_password	hc_weakpwd_weblogic	Weak password-Weblogic 12c login weak password detection
weak_password	hc_weakpwd_win_sys	Weak password - Windows system login weak password baseline

Status codes of security logs

Status code	Description
1	Unfixed.
2	Fixing failed.
3	Rollback failed.
4	Fixing.
5	Rolling back.
6	Verifying.
7	Fixed.
8	Fixed and to be restarted.

Status code	Description
9	Rolled back.
10	Ignored.
11	Rolled back and to be restarted.
12	No longer exists.
20	Expired.

Status codes of alerts

Status code	Description
1	Unhandled.
2	Ignored.
4	Confirmed.
8	Marked as false positives.
16	Handling.
32	Handled.
64	Expired.
128	Deleted.
512	Automatic blocking.
513	Automatically blocked.

Status codes of baseline logs

Status code	Description
1	Baseline checks failed.
2	Verifying.
3	Baseline checks passed.
5	Expired.
6	Ignored.
7	Fixing.

Alert logs

Field name	Description	Example
data_source	The data source. For more information, see Data source of alerts.	aegis_login_log
level	The severity of the alert event. The following valid values are listed in descending order: • serious • suspicious • remind	suspicious
name	The name of the alert.	Suspicious Process-SSH-based Remote Execution of Non-interactive Commands
op	The operation. Valid values: • new • dealing	new
status	The information about the status. For more information, see Status codes of security logs.	1
uuid	The UUID of the server on which the alert is generated.	12345-b7ca-4a0a-9267-123456
detail	The details of the alert. Note The content of the detail field in the log varies based on the alert type. If you have questions about the parameters in the detail field when you view alert logs, you can for consultation.	The content of the detail field is long. The following content is extracted from the detail field in an alert log that is generated for an unapproved location logon to a server: {"loginSourceIp":"120.27.XX.XX","loginTimes":1,"type":"login_common_location","loginDestinationPort":22,"loginUser":"aike","protocol":2,"protocolName":"SSH","location":"Qingdao"}
unique_info	The ID of the alert.	2536dd765f804916a1fa3b9516b5****

Data source of alerts

Value	Description
aegis_suspicious_event	Host exceptions
aegis_suspicious_file_v2	Webshell
aegis_login_log	Unusual logons
security_event	Security Center exceptions

Value	Description

Host logs

Process startup logs

Field name	Description	Example
uuid	The UUID of the server where the process runs.	5d83b26b-b7ca-4a0a-9267-12****
ip	The IP address of the client host.	1.2.XX.XX
cmdline	The complete command to start the process.	cmd.exe /C "netstat -ano"
username	The username.	administrator
uid	The ID of the user.	123
pid	The ID of the process.	7100
filename	The name of the process file.	cmd.exe
filepath	The full path of the process file.	C:/Windows/SysWOW64/cmd.exe
groupname	The name of the user group.	group1
ppid	The ID of the parent process.	2296
pfilename	The name of the parent process file.	client.exe
pfilepath	The full path of the parent process file.	D:/client/client.exe
		"[{ ""9883"":""bash -c kill -0 -- -'6274'"" }, { ""19617"":""/opt/java8/bin/java -Dproc_nodemanager -Xmx8192m -Dhdp.version=2.6.XX.XX-292 -Dhadoop.log.dir=/var/log/hadoop-yarn/yarn -Dyarn.log.dir=/var/log/hadoop-yarn/yarn -Dhadoop.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -

Field name	Description	Example
cmd_chain	The process chain.	Dyarn.home.dir= -Dyarn.id.str=yarn -Dhadoop.root.logger=INFO,EWMA,RFA -Dyarn.root.logger=INFO,EWMA,RFA -Djava.library.path=:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir -Dyarn.policy.file=hadoop-policy.xml -Djava.io.tmpdir=/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir -server -Dnm.audit.logger=INFO,NMAUDIT -Dnm.audit.logger=INFO,NMAUDIT -Dhadoop.log.dir=/var/log/hadoop-yarn/yarn -Dyarn.log.dir=/var/log/hadoop-yarn/yarn -Dhadoop.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.log.file=yarn-yarn-nodemanager-s-tencentyun-10-54-42-64.hx.log -Dyarn.home.dir=/usr/hdp/2.6.XX.XX-292/hadoop-yarn -Dhadoop.home.dir=/usr/hdp/2.6.XX.XX-292/hadoop -Dhadoop.root.logger=INFO,EWMA,RFA -Dyarn.root.logger=INFO,EWMA,RFA -Djava.library.path=:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native/Linux-amd64-64:/usr/hdp/2.6.XX.XX-292/hadoop/lib/native:/var/lib/ambari-agent/tmp/hadoop_java_io_tmpdir -classpath /usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/conf:/usr/hdp/2.6.XX.XX-292/hadoop/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-hdfs/./:/usr/hdp/2.6.XX.XX-

Field name	Description	Example
		292/hadoop-hdfs/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-hdfs/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-mapreduce/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop-mapreduce/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/.//*:/usr/hdp/2.6.XX.XX-292/hadoop-yarn/lib/*:/usr/hdp/2.6.XX.XX-292/hadoop/conf/nm-config/log4j.properties org.apache.hadoop.yarn.server.nodemanager.NodeManager"" }] "
containerhostname	The name of the server in the container.	gamify-answer-bol-5-6876d5dc78-vf****
containerpid	The ID of the process in the container.	0
containerimageid	The ID of the image.	sha256:7fee4a991f7c41c5511234dfea37a2a5c70c894fa7b4ca5c08d9fad74077****
containerimagename	The name of the image.	registry-vpc.cn-north-2-gov-1.aliyuncs.com/lippi-dingtalk/gamify-answer-bol-start:2020111714****
containername	The name of the container.	k8s_gamify-answer-bol_gamify-answer-bol-5-6876d5dc78-vf6rb_study-gamify-answer-bol_483a1ed1-28b7-11eb-bc35-00163e010b62_0****
containerid	The ID of the container.	b564567427272d46f9b1cc4ade06a85fdf55075c06fdb870818d5925fa86****
cmd_chain_index	The index of the process chain. You can use an index to search for process chains.	P253
cmd_index	The index of a parameter in the command line. Every two indexes are grouped to identify the start of a parameter and the end of the parameter.	0,3,5,8

Field name	Description	Example
comm	The command name related to the process.	N/A
gid	The ID of the process group.	0
parent_cmd_line	The command line of the parent process.	/bin/sh -c ip a |grep inet|grep -v inet6|grep -v 127.0.0.1|grep -v 'inet 192.168.'|grep -v 'inet 10.'|awk '{print $2}'|sed 's#/[0-9]*##g'
pid_start_time	The time when the parent process was started.	2022-01-12 15:27:46
srv_cmd	The command line of the ancestor process.	/www/server/panel/pyenv/bin/python /www/server/panel/BT-Task
stime	The time when the process was started.	2022-01-12 15:27:46

Process snapshots

Field name	Description	Example
uuid	The UUID of the server where the process runs.	5d83b26b-b7ca-4a0a-9267-12****
ip	The IP address of the client host.	1.2.XX.XX
cmdline	The complete command to start the process.	cmd.exe /C "netstat -ano"
pid	The ID of the process.	7100
name	The name of the process file.	cmd.exe
path	The full path of the process file.	C:/Windows/SysWOW64/cmd.exe
md5	The MD5 hash value of the process file. **Note** The MD5 algorithm is not supported for files that exceed 1 MB.	d0424c22dfa03f6e4d5289f7f5934dd4
pname	The name of the parent process file.	client.exe
start_time	The time when the process was started. This field is built-in.	2018-01-18 20:00:12
user	The username.	administrator

Field name	Description	Example
uid	The ID of the user.	123

Logon logs

> **Note** The repeated logon attempts within 1 minute are recorded in one log. The `warn_count` field indicates the number of logon attempts.

Field name	Description	Example
uuid	The UUID of the server that is logged on to.	5d83b26b-b7ca-4a0a-9267-12****
ip	The IP address of the client host.	1.2.XX.XX
warn_ip	The source IP address.	1.2.XX.XX
warn_port	The logon port.	22
warn_type	The logon type. Valid values: • SSHLOGIN: Secure Shell (SSH) logon • RDPLOGIN: remote desktop logon • IPCLOGIN: Internet Process Connection (IPC) connection logon	SSHLOGIN
warn_user	The username that is used for the logon.	admin
warn_count	The number of logon attempts. The repeated logon attempts within 1 minute are recorded in one log. For example, if the value of the `warn_count` field is 3, three logon attempts were performed within one minute.	3

Brute-force attack logs

Field name	Description	Example
uuid	The UUID of the server that is under a brute-force attack.	5d83b26b-b7ca-4a0a-9267-12*****
ip	The IP address of the server.	1.2.XX.XX
warn_ip	The source IP address.	1.2..XX.XX

Field name	Description	Example
warn_port	The logon port.	22
warn_type	The logon type. Valid values: • SSHLOGIN: SSH logon • RDPLOGIN: remote desktop logon • IPCLOGIN: IPC connection logon	SSHLOGIN
warn_user	The username that is used for the logon.	admin
warn_count	The number of failed logon attempts.	3

Network connection logs

Note Changes in network connections are collected by the server every 10 seconds to 1 minute. The changes are collected from the time when a connection is established to the time when the connection ends.

Field name	Description	Example
uuid	The UUID of the server.	5d83b26b-b7ca-4a0a-9267-12****
ip	The IP address of the server.	1.2.XX.XX
src_ip	The source IP address.	1.2.XX.XX
src_port	The source port.	41897
dst_ip	The destination IP address.	1.2.XX.XX
dst_port	The destination port.	22
proc_name	The name of the process.	java
proc_path	The path of the process.	/hsdata/jdk1.7.0_79/bin/java
proto	The protocol. Valid values: • tcp • udp • raw, which indicates raw socket	tcp
status	The status of the network connection. For more information, see Status codes of network connections.	5

Field name	Description	Example
cmd_chain	The process chain.	{ "9883":"bash -c kill -0 -- - '6274'" }, { "19617":"/opt/java8/bin/java - Dproc_nodemanager -Xmx8192m - Dhdp.version=2.6.5.0-292 - Dhadoop.log.dir=/var/log/hadoop- yarn/yarn - Dyarn.log.dir=/var/log/hadoop-yarn/yarn -Dhadoop.log.file=yarn-yarn-nodemanager- s-tencentyun-10-54-42-64.hx.log - Dyarn.log.file=yarn-yarn-nodemanager-s- tencentyun-10-54-42-64.hx.log - Dyarn.home.dir= -Dyarn.id.str=yarn - Dhadoop.root.logger=INFO,EWMA,RFA - Dyarn.root.logger=INFO,EWMA,RFA - Djava.library.path=:/usr/hdp/2.6.5.0- 292/hadoop/lib/native/Linux-amd64- 64:/usr/hdp/2.6.5.0- 292/hadoop/lib/native/Linux-amd64- 64:/usr/hdp/2.6.5.0- 292/hadoop/lib/native:/var/lib/ambari- agent/tmp/hadoop_java_io_tmpdir:/usr/hdp /2.6.5.0-292/hadoop/lib/native/Linux- amd64-64:/usr/hdp/2.6.5.0- 292/hadoop/lib/native/Linux-amd64- 64:/usr/hdp/2.6.5.0- 292/hadoop/lib/native:/var/lib/ambari- agent/tmp/hadoop_java_io_tmpdir - Dyarn.policy.file=hadoop-policy.xml - Djava.io.tmpdir=/var/lib/ambari- agent/tmp/hadoop_java_io_tmpdir -server -Dnm.audit.logger=INFO,NMAUDIT - Dnm.audit.logger=INFO,NMAUDIT - Dhadoop.log.dir=/var/log/hadoop- yarn/yarn - Dyarn.log.dir=/var/log/hadoop-yarn/yarn -Dhadoop.log.file=yarn-yarn-nodemanager- s-tencentyun-10-54-42-64.hx.log - Dyarn.log.file=yarn-yarn-nodemanager-s- tencentyun-10-54-42-64.hx.log - Dyarn.home.dir=/usr/hdp/2.6.5.0- 292/hadoop-yarn - Dhadoop.home.dir=/usr/hdp/2.6.5.0- 292/hadoop - Dhadoop.root.logger=INFO,EWMA,RFA - Dyarn.root.logger=INFO,EWMA,RFA - Djava.library.path=:/usr/hdp/2.6.5.0- 292/hadoop/lib/native/Linux-amd64- 64:/usr/hdp/2.6.5.0-

Field name	Description	Example
		292/hadoop/lib/native/Linux-amd64- 64:/usr/hdp/2.6.5.0- 292/hadoop/lib/native:/var/lib/ambari- agent/tmp/hadoop_java_io_tmpdir:/usr/hdp /2.6.5.0-292/hadoop/lib/native/Linux- amd64-64:/usr/hdp/2.6.5.0- 292/hadoop/lib/native/Linux-amd64- 64:/usr/hdp/2.6.5.0- 292/hadoop/lib/native:/var/lib/ambari- agent/tmp/hadoop_java_io_tmpdir - classpath /usr/hdp/2.6.5.0- 292/hadoop/conf:/usr/hdp/2.6.5.0- 292/hadoop/conf:/usr/hdp/2.6.5.0- 292/hadoop/conf:/usr/hdp/2.6.5.0- 292/hadoop/lib/*:/usr/hdp/2.6.5.0- 292/hadoop/.//*:/usr/hdp/2.6.5.0- 292/hadoop-hdfs/./:/usr/hdp/2.6.5.0- 292/hadoop-hdfs/lib/*:/usr/hdp/2.6.5.0- 292/hadoop-hdfs/.//*:/usr/hdp/2.6.5.0- 292/hadoop-yarn/lib/*:/usr/hdp/2.6.5.0- 292/hadoop-yarn/.//*:/usr/hdp/2.6.5.0- 292/hadoop- mapreduce/lib/*:/usr/hdp/2.6.5.0- 292/hadoop- mapreduce/.//*:/usr/hdp/2.6.5.0- 292/hadoop-yarn/.//*:/usr/hdp/2.6.5.0- 292/hadoop-yarn/lib/*:/usr/hdp/2.6.5.0- 292/hadoop/conf/nm- config/log4j.properties org.apache.hadoop.yarn.server.nodemanage r.NodeManager" }]
pid	The ID of the process.	123
ppid	The ID of the parent process.	1
container_host name	The name of the server in the container.	gamify-answer-bol-5-6876d5dc78-v****
container_pid	The ID of the process in the container.	0
container_ima ge_id	The ID of the image.	sha256:7fee4a991f7c41c5511234dfea37a2a5c70c89 4fa7b4ca5c08d9fad74077****
container_ima ge_name	The name of the image.	registry-vpc.cn-north-2-gov-1.aliyuncs.com/lippi-dingtalk/gamify-answer-bol-start:2020111714****

Field name	Description	Example
container_name	The name of the container.	k8s_gamify-answer-bol_gamify-answer-bol-5-6876d5dc78-vf6rb_study-gamify-answer-bol_483a1ed1-28b7-11eb-bc35-00163e010b62_0****
container_id	The ID of the container.	b564567427272d46f9b1cc4ade06a85fdf55075c06fdb870818d5925fa86****
cmd_chain_index	The index of the process chain. An index can be used to search for process chains.	P3285
parent_proc_file_name	The name of the parent process file.	/usr/bin/bash
proc_start_time	The time when the process was started.	N/A
srv_comm	The command name related to the ancestor process.	python
uid	The ID of the user who started the process.	-1
username	The name of the user who started the process.	N/A

Status codes of network connections

Status code	Description
1	closed
2	listen
3	syn send
4	syn recv
5	establisted
6	close wait
7	closing
8	fin_wait1
9	fin_wait2
10	time_wait
11	delete_tcb

Snapshots of port listening

Field name	Description	Example
uuid	The UUID of the server.	5d83b26b-b7ca-4a0a-9267-12****
ip	The IP address of the server.	1.2.XX.XX
proto	The communication protocol. Valid values: • tcp • udp • raw, which indicates raw socket	tcp
src_ip	The IP address of the listener.	1.2.XX.XX
src_port	The listener port.	41897
pid	The ID of the process.	7100
proc_name	The name of the process.	kubelet

Account snapshots

Note The account snapshots contain information about the accounts that are detected in your assets.

Field name	Description	Example
uuid	The UUID of the server.	5d83b26b-b7ca-4a0a-9267-12****
ip	The IP address of the server.	1.2.XX.XX
user	The name of the user.	nscd
perm	Indicates whether you can log on to the server as a root user. Valid values: • 0: no • 1: yes	0
home_dir	The home directory.	/Users/abc
groups	The group to which the user belongs. The value `N/A` indicates that the user does not belong to any group.	["users", "root"]
last_chg	The date when the password was last modified.	2017-08-24

Field name	Description	Example
shell	The Linux shell command.	/sbin/nologin
domain	The Windows domain. The value `N/A` indicates that the user does not belong to a domain.	administrator
tty	The terminal that is logged on to. The value `N/A` indicates that the account has not been used for terminal logon.	pts/3
warn_time	The date when you are notified of expiring passwords. The value `never` indicates that notifications are disabled.	2017-08-24
account_expire	The date when the account expires. The value `never` indicates that the account never expires.	2017-08-24
passwd_expire	The date when the password expires. The value `never` indicates that the account never expires.	2017-08-24
login_ip	The IP address from which the last remote logon was initiated. The value `N/A` indicates that the account has not been used for logons.	1.2.XX.XX
last_logon	The date and time of the last logon. The value `N/A` indicates that the account has not been used for logons.	2017-08-21 09:21:21
status	The status of the account. Valid values: • 0: Logons from the account are not allowed. • 1: Logons from the account are allowed.	0

1.5. Real-time log analysis

1.5.1. Use custom log query and analysis

On the Log Analysis page of the Security Center console, you can perform custom log queries and analysis in multiple complex scenarios. This topic describes the syntax for query and analysis statements.

Overview

In the Security Center console, choose **Investigation > Log Analysis** and enter SQL statements in **Search & Analyze** to perform custom log queries and analysis. A log query statement consists of two parts: search syntax and analytics syntax, divided by vertical bars (|).

You can perform custom log queries and analysis without the need to specify the search syntax or analytics syntax. The following list describes the search syntax and analytics syntax:

- Search: You can use keywords, fuzzy match conditions, numeric values, ranges, or combinations to generate search conditions. If the value of the Search part is an asterisk (*) or is empty, data from the specified period is not filtered. In this case, all data from the specified period is used for analysis.
- Analytics: It calculates and collects statistics on search results or full data. If the value of the Analytics part is empty, the results of the query are returned but no statistics are calculated.

Search syntax

The search syntax of Log Service supports both full-text query and field query. The query box supports features such as multi-line search and syntax highlighting.

- **Full-text query**

  You can enter keywords to search for logs without the need to specify fields. To use multiple keywords, enclose each keyword within a pair of quotation marks (`"`) and separate them with spaces or the operator `and`. Examples:

  - **Query with multiple keywords specified**

    Search for the logs that contain `www.aliyundoc.com` and `404`. Examples:

    ```
    www.aliyundoc.com 404
    ```

    or:

    ```
    www.aliyundoc.com and 404
    ```

  - **Conditional query**

    Search for the logs that contain `www.aliyundoc.com` and `error`, or the logs that contain www.aliyundoc.com and `404`. Example:

    ```
    www.aliyundoc.com and (error or 404)
    ```

  - **Suffix-based query**

    Search for the logs that contain `www.aliyundoc.com` and start with `failed_`. Example:

    ```
    www.aliyundoc.com and failed_*
    ```

    > **Note** A full-text query supports only suffixes with asterisks (`*`). Prefixes with asterisks (`*`) are not supported.

- **Field query**

  Data of numeric fields can be filtered by using `Field:Value` or `Field≥Value`. You can combine the two formats by using `and` or `or`. It can also be used with a full-text query by using the combination specified by `and` and `or`.

  Log Service supports more accurate queries based on fields.

  - **Multi-field query**

    Search for alert logs whose severity level is **serious**. Example:

    ```
    __topic__ : sas-security-log and level: serious
    ```

    Search for all SSH logons on the client whose IP address is 1.2.XX.XX. Example:

    ```
    __topic__:aegis-log-login and ip:1.2.XX.XX and warn_type:SSHLOGIN
    ```

    > **Note** Each log contains the `__topic__` field that indicates a log topic. Logs are distinguished by this field. In these examples, the fields, such as `level`, `warn_type`, and `ip`, are the fields for specific types of logs.

  - **Numeric field query**

    Search for all internal DNS query logs that have a response time of more than 1 second. Example:

    ```
    __topic__:local-dns and time_usecond > 1000000
    ```

    Range-based queries are also supported. For example, you can use range-based queries to search for internal DNS logs with a response time that is greater than 1 second but less than or equal to 10 seconds. Example:

    ```
    __topic__:local-dns and time_usecond in [1000000,10000000]
    ```

  For more information about the syntax, see Log search overview.

Analytics syntax

You can use SQL-92 statements to analyze and collect statistics on logs. For more information about the syntax and functions supported by Log Service, see Log analysis overview.

The `FROM` tablename clause in the standard SQL syntax can be omitted from analytics statements. This means that the `FROM LOG` clause can be omitted.

By default, Log Service returns the first 100 log entries. You can modify the number of log entries to return by using the LIMIT syntax. For more information, see LIMIT clause.

Time-based log query and analysis

Each log entry has a built-in field `__time__`, which indicates the time at which this log is generated. This field facilitates time-based statistical analysis. The value of the field is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC. Therefore, a timestamp must be converted into a supported format before it can be displayed.

- **Select and display the time**

In this example, query the last 10 logon logs with the IP address of `1.2.XX.XX` within a specific time range. The return value includes the time, source IP address, and logon type. Example:

```
__topic__: aegis-log-login and ip: 1.2.XX.XX
| select date_format(__time__, '%Y-%m-%d %H:%i:%s') as time, warn_ip, warn_type
order by __time__ desc
limit 10
```

- **Calculate the time**

  Use `__time__` to calculate the number of days after the logon. Example:

```
__topic__: aegis-log-login and ip: 1.2.XX.XX
| select date_format(__time__, '%Y-%m-%d %H:%i:%s') as time, warn_ip, warn_type ,
round((to_unixtime(now()) - __time__)/86400,1) as "days_passed"
order by __time__ desc
limit 10
```

  In this example, `round((to_unixtime(now()) - __time__)/86400, 1)` is used to perform the calculation. First, the function uses `to_unixtime` to convert the time returned by `now()` to a UNIX timestamp. Second, it subtracts the built-in `__time__` field from the calculated value to obtain the number of seconds that have elapsed. Then, the function divides the calculated value by 86400, which is the total number of seconds in a day. Finally, the `round(data, 1)` function rounds the obtained value to one decimal place to calculate the number of days that have passed since the generation of each attack log.

- **Group statistics based on a specific time**

  If you want to know the logon trends for a device within a specific time range, execute the following SQL statement:

```
__topic__: aegis-log-login and ip: 1.2.XX.XX
| select date_trunc('day', __time__) as dt,
count(1) as PV
group by dt
order by dt
```

  The built-in `__time__` field is passed to the `date_trunc('day', ..)` function to align the time by day. Each log entry is grouped into the partition of the day to which it belongs to facilitate the calculation of the total number `(count(1))`. The log entries are sorted by partition time block. You can use other values for the first parameter of the `date_trunc` function to group log entries based on other time units, such as `second`, `minute`, `hour`, `week`, `month`, and `year`. For more information about the function, see Date and time functions.

- **Group statistics based on a flexible time**

  If you want to know more flexible rules of time grouping, such as logon trends per 5 minutes for devices of your account, execute the following SQL statement:

```
__topic__: aegis-log-login
| select from_unixtime(__time__ - __time__% 300) as dt,
count(1) as PV
group by dt
order by dt
limit 1000
```

In this example, the built-in time field is used to calculate `__time__ - __time__% 300` and the `from_unixtime` function is used for formatting. Each log entry is grouped into a 5-minute (300 seconds) partition to facilitate the calculation of the total number `(count(1))`. The log entries are sorted by partition time block to obtain the first 1,000 log entries, which is equivalent to selecting data in the first 83 hours.

For more information about time-related functions, see Date and time functions. For example, the `date_parse` and `date_format` functions can convert a time format to another format.

Client IP address-based log query and analysis

The `warn_ip` field in a logon log entry indicates the source IP address of the logon.

- Source country distribution of logons

  Query the distribution of the source countries from which users log on to a server. Example:

  ```
  __topic__: aegis-log-login and uuid: 12344567
  | SELECT ip_to_country(warn_ip) as country,
  count(1) as "Number of logons"
  group by country
  ```

  In this example, the `ip_to_country` function is used to retrieve the country that corresponds to `warn_ip`, which specifies the source IP address of the logon.

- Identity distribution of logons

  Use the `ip_to_province` function to retrieve a more detailed distribution of logons based on provinces. Example:

  ```
  __topic__: aegis-log-login and uuid: 12344567
  | SELECT ip_to_province(warn_ip) as province,
           count(1) as "Number of logons"
           group by province
  ```

  In this example, the `ip_to_province` function is used to retrieve the source province to which an IP address belongs. If the IP address is not from China, the system attempts to convert it to the province or state based on the country location of the IP address. However, if you select the China map, the province or state cannot be displayed.

- Geothermal distribution of logons

  Use the `ip_to_geo` function to retrieve the geothermal distribution of logons:

  ```
  __topic__: aegis-log-login and uuid: 12344567
  | SELECT ip_to_geo(warn_ip) as geo,
           count(1) as "Number of logons"
           group by geo
           limit 10000
  ```

  In this example, the `ip_to_geo` function is used to retrieve the latitude and longitude of an IP address. LIMIT is set to 10000 to retrieve the first 10,000 log entries.

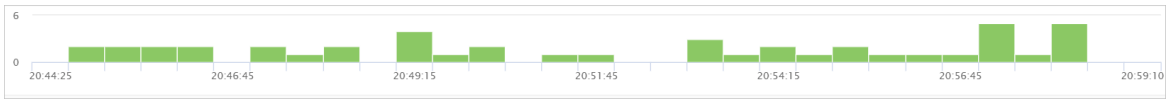
> **Note** For more information about IP address-based features, see IP functions. For example, you can use the `ip_to_provider` function to obtain the provider of IP addresses and the `ip_to_domain` function to determine whether an IP address is public or private.

1.5.2. View the distribution of logs within a specific time range

You can view the distribution of logs within a specific time range on the Log Analysis page. The distribution is displayed in a column chart. This topic describes how to view the distribution of logs within a specific time range.

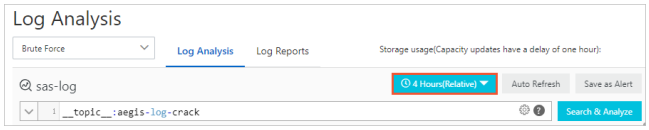
Procedure

1.
2.
3. On the **Log Analysis** page, view the distribution of logs within a specific time range.



The column chart displays the log trends on the dates that you want to query and the total number of logs queried. The x-axis displays the time. The y-axis displays the number of logs that are queried. You can perform the following operations:

- Click a column in the chart to narrow the selected time range and display the query results in the selected time range.
- In the upper-right corner, click the time picker and select the time range in which you want to view logs.

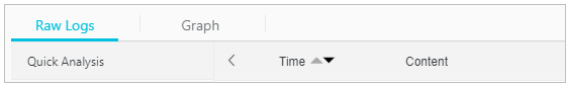


1.5.3. View raw logs

You can use the log analysis feature to view raw logs and their details. You can download raw logs to your computer.

Context

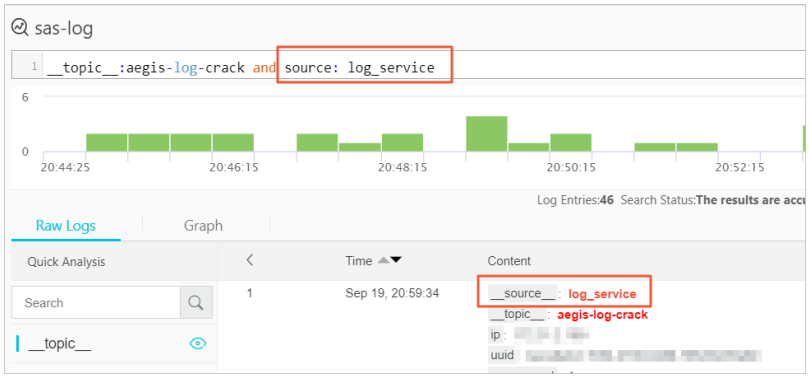
The **Raw Logs** tab shows the details of each log entry, including time, content, and fields. For more information about log fields, see Log fields.



Procedure

1.
2.

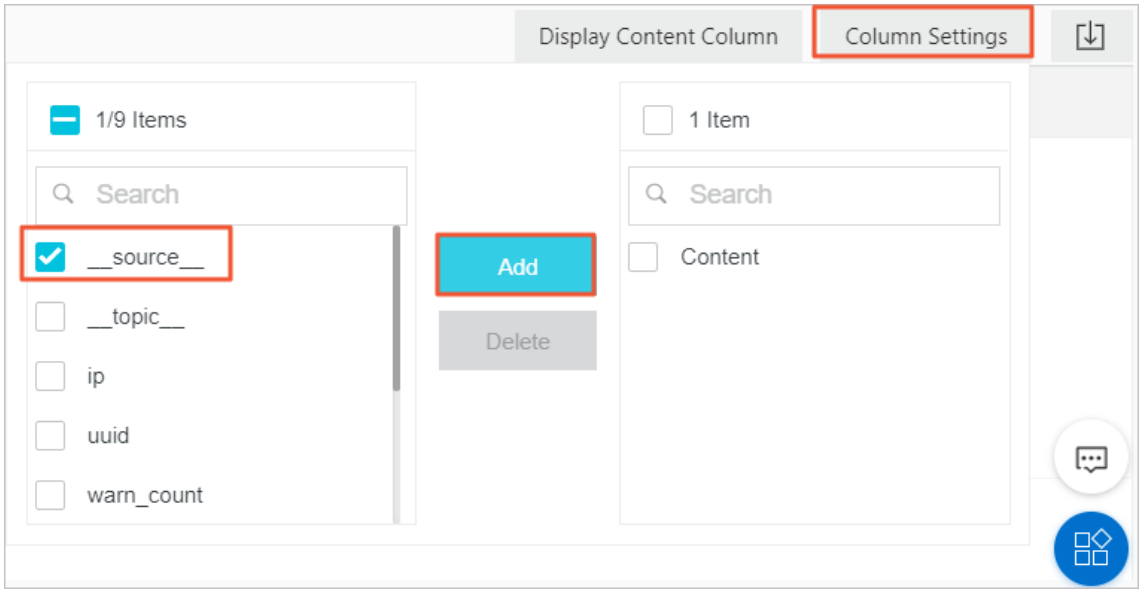
3. On the **Raw Logs** tab, click a field in the **Content** column to automatically add the field to the search box.



> **Note** For example, after you click **log_service**, this field is added to the search box. You can click **Search & Analyze** to view the logs related to this field.

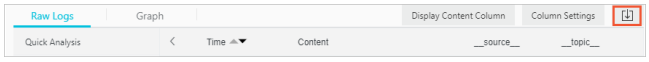
You can perform the following operations on the **Raw Logs** tab:

- In the upper-right corner of the **Raw Logs** tab, click **Column Settings** to add the required fields to the raw log list.

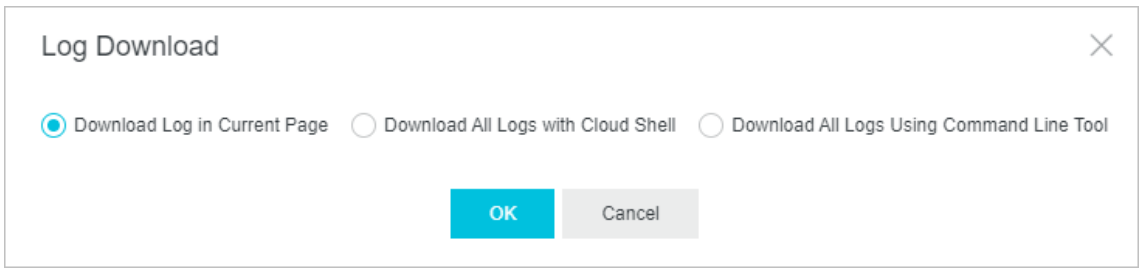


After the fields are added, the raw log list displays the fields as columns.

- Click the icon next to **Column Settings**. The **Log Download** dialog box appears.



In the Log Download dialog box, you can select **Download Log in Current Page**, **Download All Logs with Cloud Shell**, or **Download All Logs Using Command Line Tool** and click **OK** to download the logs.



- **Download Log in Current Page**: Download the logs of the current page to a CSV file.
- **Download All Logs with Cloud Shell**: Automatically download all logs. For more information, see Export log data.
- **Download All Logs Using Command Line Tool**: Use the command-line tool to download all logs. For more information, see Export logs.

1.5.4. View graphs

The log analysis feature visualizes the log analysis results in graphs.

On the **Graph** tab of the Security Center console, you can select different graph types, add log graphs to the dashboard, or download logs.

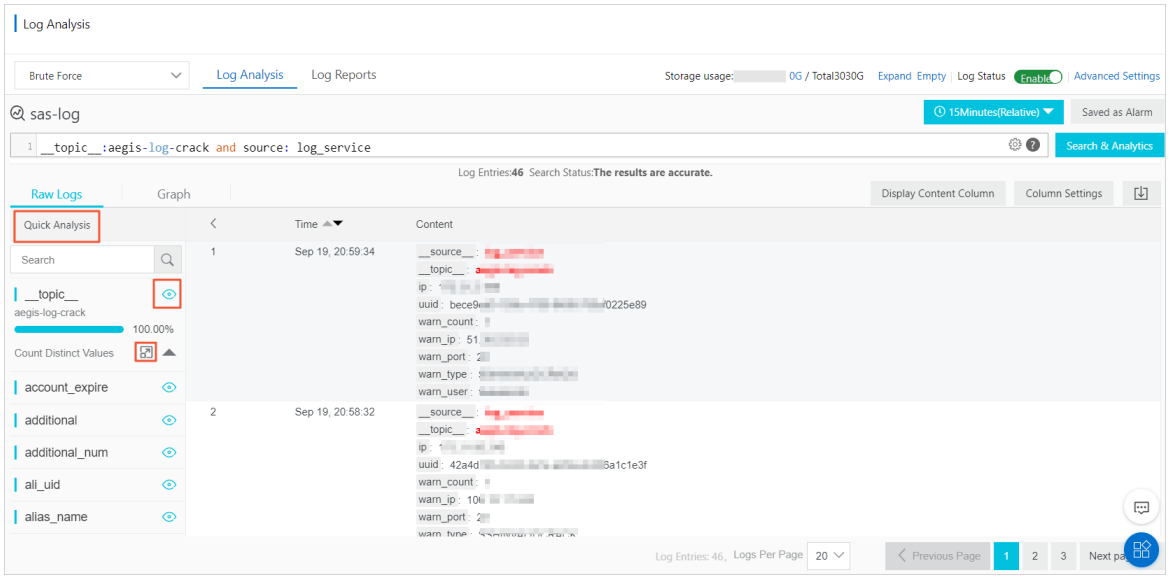
For more information about graph types, see Chart overview.

1.5.5. Perform quick analysis

The quick analysis feature provides a one-click interactive query that helps you analyze the distribution of a field over a period of time. This makes searches for crucial data more efficient.

Procedure

1.
2.
3. On the **Log Analysis** page, click the **Raw Logs** tab. In the **Quick Analysis** column, view the fields contained in logs and the ratio of each field.



You can perform the following operations:

- Click the icon to the right of a log field to view the quick analysis results.
- Click the icon in the lower-right corner of a field in the **Quick Analysis** column to add the query statement of grouping statistics to the search box for further operations. The log graphs of specific fields are also displayed.

1.5.6. Query logs

Security Center is connected to Log Service, which allows you to query and analyze 14 subtypes of logs. The logs cover network logs, host logs, and security logs. Security Center automatically collects and stores logs in real time. It is connected to Log Service to provide query, analysis, reporting, alerting, delivery, and integration with downstream computing systems.

Prerequisites

Log analysis is enabled. For more information, see Enable log analysis.

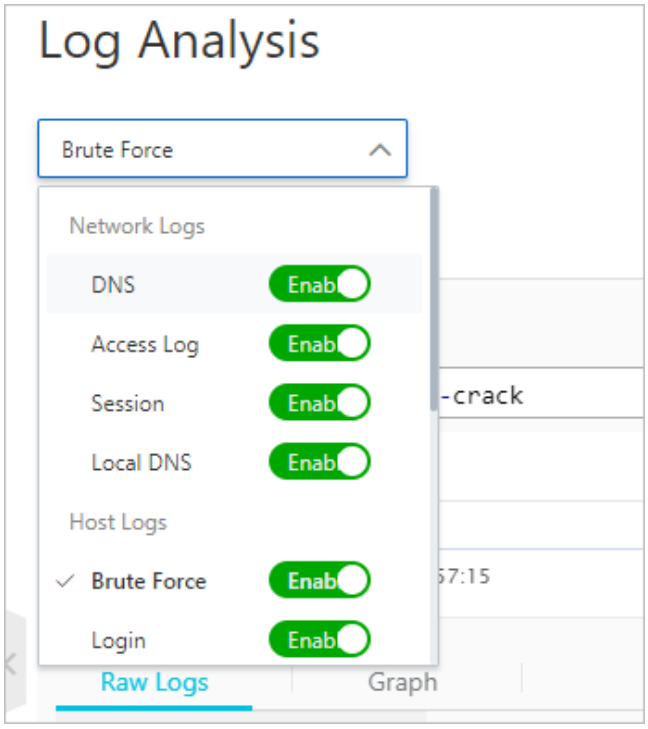
Limits

The and editions support 14 subtypes of logs while the edition supports only 10 subtypes of logs that cover host and security logs. The and editions do not support log analysis. For more information about the editions that support log analysis, see Features.

Procedure

After you select a specific type, you can query and analyze the collected logs of this type in real time. You can also perform operations, such as viewing or editing dashboards and configuring monitoring and alerting.

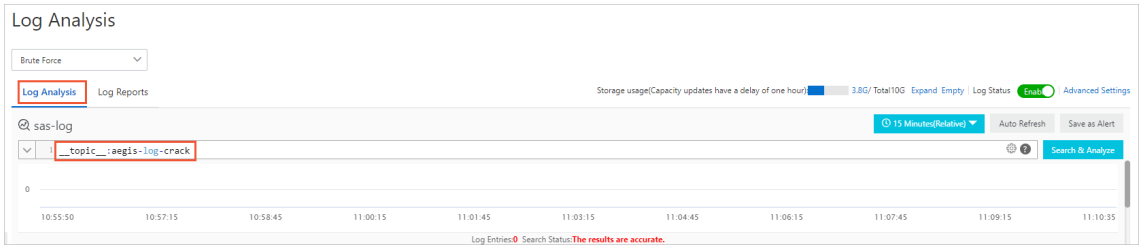
1.
2.
3. In the upper-left corner of the **Log Analysis** page, select the type of log that you want to view and set Log Status to **Enabled**.



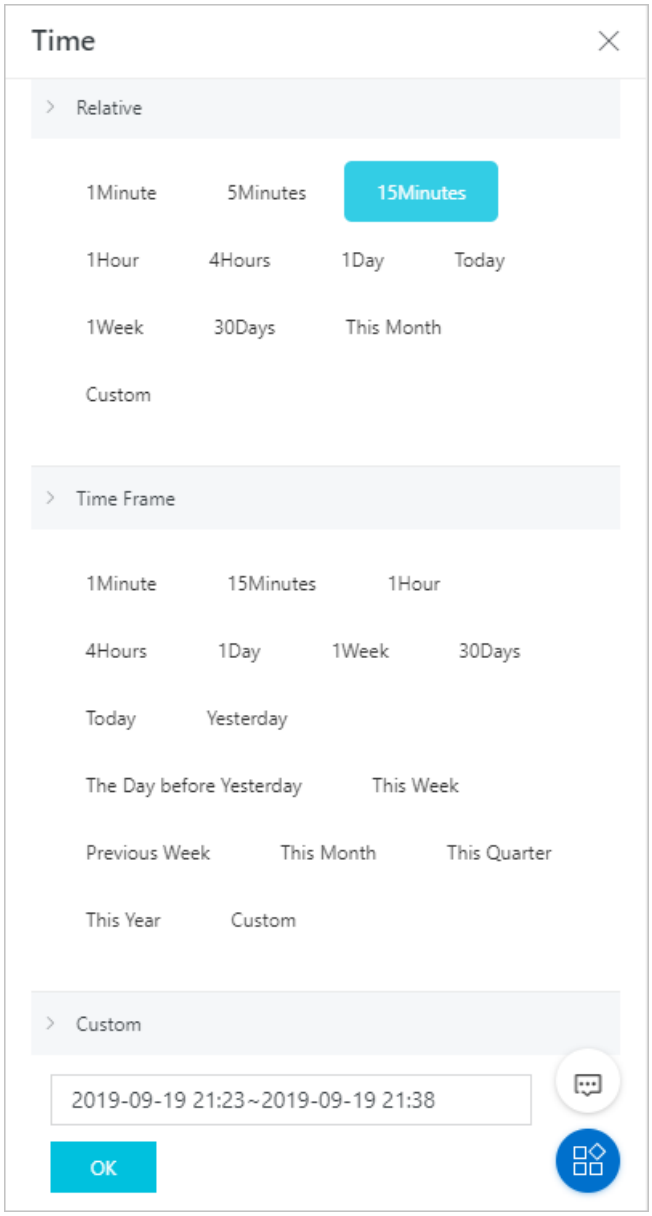
4. On the **Log Analysis** page, query and analyze logs.

   On the page:

   - The **Log Analysis** tab displays the log query and analysis results of the type that you select in Step 3. The system automatically provides query statements for you.

   - You can click the time above the **Search / Analyze** button. In the **Time** panel, specify the time range, close the panel, and then click **Search / Analyze** to view the logs in the specified time range.



Note Security Center logs can be stored for 180 days. Each log entry is deleted on the 180th day after it is generated.

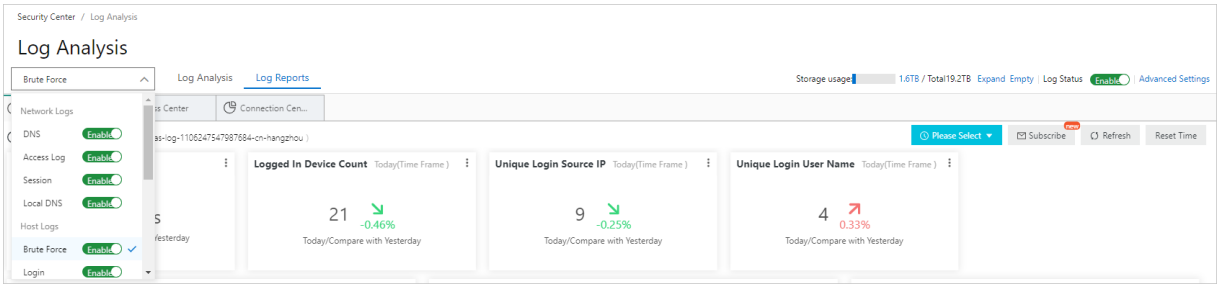
1.6. Log report dashboards

Security Center provides dashboards for network logs, host logs, and security logs on the Log Reports tab of the Log Analysis page.

After you enable the log analysis feature, Security Center automatically creates the dashboards of reports. You can view the dashboards on the **Log Reports** tab. To go to this tab, log on to the and choose **Investigation > Log Analysis**.

Log type	Log report
	DNS Access Center

Log type Network logs	Log report
	Network Session Center
	Web Access Center
Host logs	Login Center
	Process Center
	Connection Center
Security logs	Baseline Center
	Vulnerability Center
	Alarm Center



Network logs

The following log reports are provided for network logs:

- DNS Access Center

  Security Center provides an overview of domain name system (DNS) queries on the server. The overview includes the success rate of external DNS queries, and the distribution and trends of both local and external DNS queries.

Widget	Display method	Default time range	Description	Example
External DNS Traffic	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of external DNS traffic packets in a period on the current day and the change compared with the same period on the last day.	10.0, 0.01%

Widget	Display method	Default time range	Description	Example
External DNS Successful Query Ratio	Single value comparison	Today (Time Frame) and Compare with Yesterday	The success rate of external DNS queries the current day and the change compared with the last day.	100%, 0.01%
Unique DNS Queried Site	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of domain names that a unique DNS queries the current day and the change compared with the last day.	10.0, 0.01%
Local DNS Traffic	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of local DNS traffic packets the current day and the change compared with the last day.	1,000, 0.01%
External Query Device Distribution	World map	Today (Time Frame)	The geographical distribution of public network devices that are used to initiate external DNS queries.	None
External DNS Traffic Trend	Column chart and line chart	Today (Time Frame)	The trends in the number of requests and the success rate of external DNS queries per hour.	None
Local DNS Traffic Trend	Column chart	Today (Time Frame)	The trend in the number of requests for local DNS queries per hour.	None
External DNS Most Queried Site Top 20	Pie chart	Today (Time Frame)	Top 20 domain names that initiate the most external DNS queries.	None

Widget	Display method	Default time range	Description	Example
Local DNS Device with Most Query Top 20	Pie chart	Today (Time Frame)	Top 20 devices that initiate the most local DNS queries.	None
Local DNS Most Queried Site Top 20	Pie chart	Today (Time Frame)	Top 20 domain names that initiate the most local DNS queries.	None

- Network Session Center

  Security Center provides an overview of asset-related network sessions. The overview includes connection trends, connection distributions, connection destinations, access trends, and access distributions.

Widget	Display method	Default time range	Description	Example
Network Session	Single value comparison	1 Hour (Relative) and Compare with Yesterday	The number of network sessions in a period on the current day and the change compared with the same period on the last day.	10.0, -0.01%
Unique Destination IP	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of **unique destination IP addresses** for network sessions the current day and the change compared with the last day.	10.0, -0.01%
Unique Source IP	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of **unique source IP addresses** for network sessions the current day and the change compared with the last day.	10.0, 0.01%

Widget	Display method	Default time range	Description	Example
Unique Destination Port	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of **unique destination ports** for network sessions the current day and the change compared with the last day.	10.0, -0.01%
Network Connection Trend (Protocol)	Flow diagram	Today (Time Frame)	The trend in the number of network sessions by protocol, such as TCP and UDP, per hour.	None
Network Connection Trend (Asset Type)	Double line graph	Today (Time Frame)	The trend in the number of assets, such as Elastic Compute Service (ECS) instances or Server Load Balancer (SLB) instances, used by network sessions per hour.	None
Session Protocol Distribution	Pie chart	Today (Time Frame)	The distribution of network sessions by protocol, such as TCP and UDP.	None
Destination Port Top 10	Pie chart	Today (Time Frame)	The distribution of the top 10 destination ports with the most network sessions.	None
Related Asset Type Distribution	Pie chart	This Month (Time Frame)	The distribution of the types of assets associated with a network session. The assets include ECS and SLB instances.	None

Widget	Display method	Default time range	Description	Example
Destination Distribution (World)	World map	Today (Time Frame)	The geographical distribution of destination IP addresses for outbound sessions around the world.	None
Source Distribution (World)	World map	Today (Time Frame)	The geographical distribution of source IP addresses for inbound sessions around the world.	None
Destination Distribution (China)	China map	Today (Time Frame)	The geographical distribution of destination IP addresses for outbound sessions in China.	None
Source Destination (China)	China map	Today (Time Frame)	The geographical distribution of source IP addresses for inbound sessions in China.	None

- Web Access Center

  Security Center provides an overview of outbound HTTP requests and access to the web services of a host. The overview includes the request success rate, access trends, success efficiency, distribution of accessed domain names, and other related distributions.

Widget	Display method	Default time range	Description	Example
Valid Request Ratio	Single value comparison	Today (Time Frame) and Compare with Yesterday	The success rate of HTTP requests the current day and the change compared with the last day. The success rate is calculated as the percentage of returned status codes that are less than 400.	0.01%, 10.00

Widget	Display method	Default time range	Description	Example
Web Access Count	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of HTTP requests in a period on the current day and the change compared with the same period on the last day.	1,000, -0.01%
Unique Destination	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of unique destination IP addresses for HTTP requests the current day and the change compared with the last day.	10.0, -0.01%
Unique Source	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of unique source IP addresses for HTTP requests the current day and the change compared with the last day.	1,000, 0.01%
Web Access Trend and Valid Ratio	Column chart and line chart	Today (Time Frame)	The trends in the number of HTTP requests and the success rate per hour. The success rate is calculated as the percentage of returned status codes that are less than 400.	None
Unique Source/Destination Trend	Double line graph	Today (Time Frame)	The trends in the numbers of unique source IP addresses and destination IP addresses per hour.	None
Access Status Distribution	Flow diagram	Today (Time Frame)	The distribution of returned status codes, such as 2xx and 3xx, per hour.	None

Widget	Display method	Default time range	Description	Example
Accessed Site Top 10	Histogram	Today (Time Frame)	The distribution of top 10 domain names that are accessed the most.	None
Content Type Distribution Top 10	Pie chart	Today (Time Frame)	Top 10 content types, such as text and plain, that are requested the most.	None
Referer	Table	Today (Time Frame)	Top 20 referers that are referred the most. The table contains the following fields: URL, Host, and Total Count.	None

Host logs

The following log reports are provided for host logs:

- Login Center

  Security Center provides an overview of logons to hosts. The overview includes the geographical distributions of source and destination IP addresses, trends, logon ports, and logon types.

Widget	Display method	Default time range	Description	Example
Login Count	Single value comparison	1 Hour (Relative) and Compare with Yesterday	The number of logons in a period on the current day and the change compared with the same period on the last day.	10.0, 10%
Logged In Device Count	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of **unique hosts** to which are logged on the current day and the change compared with the last day.	10, -10%

Widget	Display method	Default time range	Description	Example
Unique Login Source IP	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of unique source IP addresses that are used to log on to hosts the current day and the change compared with the last day.	10, 10%
Unique Login User Name	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of unique usernames that are used to log on to hosts the current day and the change compared with the last day.	10, 10%
Login on Device Trend	Column chart and line chart	Today (Time Frame)	The trends in the number of hosts to which are logged on and the number of logons per hour.	None
Login Method Trend	Flow diagram	Today (Time Frame)	The trend in the number of logons that use different methods, such as RDP and SSH, per hour.	None
Login Method Distribution	Pie chart	4 Hours (Relative)	The distribution of different logon methods, such as RDP and SSH.	None
Device Distribution	World map	4 Hours (Relative)	The geographical distribution of logged on hosts that are assigned public IP addresses around the world.	None

Widget	Display method	Default time range	Description	Example
Login Source Distribution	World map	4 Hours (Relative)	The geographical distribution of the source IP addresses used to log on to the hosts that are assigned public IP addresses around the world.	None
Unique Source IP Distribution	World map	4 Hours (Relative)	The geographical distribution of the unique source IP addresses used to log on to the hosts that are assigned public IP addresses around the world.	None
User with Most Login Top 10	Pie chart	4 Hours (Relative)	Top 10 usernames that are most frequently used.	None
Port with Most Login Top 10	Pie chart	4 Hours (Relative)	Top 10 destination ports that are most frequently used.	None
Activated User List	Table	4 Hours (Relative)	The first 30 accounts available on the host.	None
Source IP and User with Most Login Top 30	Table	4 Hours (Relative)	Top 30 usernames that are most frequently used to log on to the host and the logon source information. The table contains the following fields: Source Network, Source IP, Login User, Login Method, Login Destination Count, and Login Count.	None

- Process Center

  Security Center provides an overview of processes on hosts. The overview includes process startup trends, process distribution, process types, and the distribution of specific Bash and Java program startups.

Widget	Display method	Default time range	Description	Example
Process Start Count	Single value comparison	1 Hour (Relative) and Compare with Yesterday	The number of process startups in a period on the current day and the change compared with the same period on the last day.	10,000, 0.01%
Related Device Count	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of **unique hosts** on which processes are started the current day and the change compared with the last day.	10.0, 0.01%
Unique Process Name Count	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of started processes that have unique names the current day and the change compared with the last day.	10.0, 0.01%
Device Count	Column chart and line chart	Today (Time Frame)	The trends in the number of hosts on which processes are started and the number of unique processes per hour.	None
Process Start Trend	Line graph	Today (Time Frame)	The average number of processes started on each host per hour.	None

Widget	Display method	Default time range	Description	Example
Device Distribution	World map	Today (Time Frame)	The geographical distribution of hosts on which processes are started around the world. The hosts must be assigned public IP addresses.	None
Process Start Count Distribution on Device	World map	Today (Time Frame)	The geographical distribution of the process events on hosts that are assigned public IP addresses around the world.	None
Most Started Process Top 20	Table	Today (Time Frame)	Top 20 processes that are most frequently started. The table contains the following fields: Process Name, Process Path, and Start Count.	None
Process that Started Most Bash Top 20	Table	Today (Time Frame)	Top 20 processes that initiate Bash the most. The table contains the Parent Process and Start Count fields.	None
Java File with Most Start Count Top 30	Table	Today (Time Frame)	Top 30 Java files that initiate the most processes. The table contains the following fields: Jar File Name, Jar File Path, and Start Count.	None

Widget	Display method	Default time range	Description	Example
Device with Most Process Started Top 30	Table	Today (Time Frame)	Top 30 clients that initiate the most processes. The table contains the following fields: Device, Total Started Process Count, Most Started Command Line, Related Process, Start Count, and Ratio.	None

- Connection Center

  Security Center provides an overview of the connection changes for hosts. The overview includes the connection distributions, connection trends, destinations, access trends, and access distributions.

Widget	Display method	Default time range	Description	Example
Connection Event	Single value comparison	1 Hour (Relative) and Compare with Yesterday	The number of connection changes in a period on the current day and the change compared with the same period on the last day.	10.0, -0.01%
Related Device	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of **unique hosts** that have connection changes the current day and the change compared with the last day.	10.0, 0.01%
Unique Process	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of **unique processes** that have connection changes the current day and the change compared with the last day.	10.0, 0.01%

Widget	Display method	Default time range	Description	Example
Unique Source IP	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of **unique source IP addresses** that have connection changes the current day and the change compared with the last day.	10.0, 0.01%
Unique Destination IP	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of **unique destination IP addresses** that have connection changes the current day and the change compared with the last day.	1,000, 0.01%
Network Connection Trend	Double line graph	1 Hour (Relative)	The trends in the numbers of hosts on which network connection events occur and events per hour.	None
Connection Type Trend	Double line graph	1 Hour (Relative)	The trend in the distribution of connection types, such as inbound and outbound connections, involved in connection changes per hour.	None
Connection Type Distribution	Pie chart	1 Hour (Relative)	The distribution of connection types, such as inbound and outbound connections, involved in connection changes.	None

Widget	Display method	Default time range	Description	Example
Protocol Distribution	Pie chart	1 Hour (Relative)	The distribution of connection changes by protocol, such as TCP and UDP.	None
Device Distribution	World map	1 Hour (Relative)	The geographical distribution of hosts that have connection changes around the world.	None
Device Event Distribution	World map	1 Hour (Relative)	The geographical distribution of connection changes on hosts that are assigned public IP addresses around the world.	None
Connection Out Destination Distribution	World map	1 Hour (Relative)	The geographical distribution of the destination IP addresses for outbound connections involved in connection changes around the world.	None
Connection In Source Distribution	World map	1 Hour (Relative)	The geographical distribution of the source IP addresses for inbound connections involved in connection changes around the world.	None

Widget	Display method	Default time range	Description	Example
Device with Most Connection Out Top 30	Table	1 Hour (Relative)	Top 30 devices that have the most changes in outbound connections. The table contains the following fields: Device, Connection Out Count, Connection Destination Count, Related Remote Destination Port Count, and Destination Port Sample.	None
Device with Most Connection In Top 30	Table	1 Hour (Relative)	Top 30 devices that have the most changes in inbound connections. The table contains the following fields: Device, Listen IP, Connection In Count, Listen Port Count, and Port Sample.	None
Device with Most Connection Out Target Top 30	Table	1 Hour (Relative)	Top 30 devices that have the most destinations of outbound connection changes. The table includes the following fields: Device, Connection Out Count, Connection Destination Count, Connection Destination Sample, and Destination Port Sample.	None

Widget	Display method	Default time range	Description	Example
Ports with Most Connection In Top 30	Table	1 Hour (Relative)	Top 30 listener ports that have the most changes in inbound connections. The table includes the following fields: Listen Port, Connection In Count, and Process Sample.	None
Process with Most Connection Out Top 30	Table	1 Hour (Relative)	Top 30 processes that have the most changes in outbound connections. The table contains the following fields: Process Name, Connection Event Count, Related Device Count, and Path Sample.	None
Process with Most Connection In Top 30	Table	1 Hour (Relative)	Top 30 processes that have the most inbound connection changes. The table contains the following fields: Process Name, Connection Event Count, Related Device Count, and Path Sample.	None

Security logs

The following log reports are provided for security logs:

- Baseline Center

  Security Center provides an overview of baseline issues. The overview includes the distribution of baseline issues, the trend of newly occurred issues, the trend of handled issues, and issue states.

Widget	Display method	Default time range	Description	Example

Widget	Display method	Default time range	Description	Example
Related Device	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of **unique hosts** that have baseline issues the current day and the change compared with the last day.	10.0, 0.01%
New Baseline	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of new baseline issues the current day and the change compared with the last day.	10.0, -0.01%
Verify Baseline	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of verified baseline issues the current day and the change compared with the last day.	10.0, -0.01%
High Level Baseline	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of high-priority baseline issues the current day and the change compared with the last day.	10.0, 0.01%
Baseline Operation Trend	Flow diagram	Today (Time Frame)	The trend in the number of operations on baseline issues, such as operations on new issues and issue verification, per hour.	None
Baseline Subtype Trend	Flow diagram	Today (Time Frame)	The trend in the number of baseline subtypes, such as system account security and registries, per hour.	None

Widget	Display method	Default time range	Description	Example
Baseline Status Trend	Flow diagram	Today (Time Frame)	The trend in the number of baseline issues in each state, such as unfixed and fixed, per hour.	None
Baseline Operation Distribution	Doughnut chart	Today (Time Frame)	The distribution of operations on baseline issues, such as operations on new issues and issue verification.	None
Baseline Subtype Distribution	Doughnut chart	Today (Time Frame)	The distribution of baseline subtypes, such as system account security and registries.	None
Baseline Status Distribution	Doughnut chart	Today (Time Frame)	The distribution of the latest states of baselines issues, such as unfixed, fixed, and fix failed. **Notice** If a baseline issue has multiple states, the latest state is used.	None
New Baseline Top10	Doughnut chart	Today (Time Frame)	Top 10 baselines for which the most new issues are detected on each host.	None
Verify Baseline Top10	Doughnut chart	Today (Time Frame)	Top 10 baselines for which the most issues are verified on each host.	None

Widget	Display method	Default time range	Description	Example
Baseline Client Distribution Top20	Table	Today (Time Frame)	Top 10 hosts that have the most baseline issues. The table contains the following fields: Client, Baseline Event, New, Verify, High Level, and Medium Level.	None

- Vulnerability Center

  Security Center provides an overview of vulnerabilities. The overview includes the vulnerability distributions, trends of new, verified, and fixed vulnerabilities, and states of vulnerabilities.

Widget	Display method	Default time range	Description	Example
Related Device	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of **unique hosts** that have vulnerabilities the current day and the change compared with the last day.	10.0, 0.01%
New Vulnerability	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of new vulnerabilities the current day and the change compared with the last day.	10.0, 0.01%
Verify Vulnerability	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of verified vulnerabilities the current day and the change compared with the last day.	10.0, -0.01%
Fix Vulnerability	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of fixed vulnerabilities the current day and the change compared with the last day.	10.0, -0.01%

Widget	Display method	Default time range	Description	Example
Vulnerability Operation Trend	Flow diagram	Today (Time Frame)	The trend in the number of operations on vulnerabilities, such as operations on new vulnerabilities and vulnerability verification, per hour.	None
Vulnerability Type Trend	Flow diagram	Today (Time Frame)	The trend in the number of vulnerabilities of different types, such as Windows vulnerabilities, Linux vulnerabilities, and Web-CMS vulnerabilities, per hour.	None
Vulnerability Status Trend	Flow diagram	Today (Time Frame)	The trend in the number of vulnerabilities in different states, such as unfixed and fixed, per hour.	None
Vulnerability Operation Distribution	Doughnut chart	Today (Time Frame)	The distribution of operations on vulnerabilities, such as operations on new vulnerabilities and vulnerability verification.	None
Vulnerability Type Distribution	Doughnut chart	Today (Time Frame)	The distribution of vulnerabilities of different types, such as Windows vulnerabilities, Linux vulnerabilities, and Web-CMS vulnerabilities.	None

Widget	Display method	Default time range	Description	Example
Vulnerability Status Distribution	Doughnut chart	Today (Time Frame)	The distribution of the latest states of vulnerabilities, such as unfixed, fixed, and fix failed. **Notice** If a vulnerability has multiple states, the latest state is used.	None
New Vulnerability Top10	Doughnut chart	Today (Time Frame)	Top 10 vulnerabilities that are detected the most on each host.	None
Verify Vulnerability Top10	Doughnut chart	Today (Time Frame)	Top 10 vulnerabilities that are verified the most on each host.	None
Fix Vulnerability Top10	Doughnut chart	Today (Time Frame)	Top 10 vulnerabilities that are fixed the most on each host.	None

Widget	Display method	Default time range	Description	Example
Vulnerability Client Distribution Top20	Table	Today (Time Frame)	Top 20 hosts that have the most vulnerabilities. The table contains the following fields: Client, Vulnerability Event, New, Verify, Fix, Windows Vulnerability, Linux Vulnerability, and Web Vulnerability.	None

- Alarm Center

  Security Center provides an overview of security alerts. The overview includes the trends, distributions, and states of new and handled alerts.

Widget	Display method	Default time range	Description	Example
Related Device	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of **unique hosts** for which security alerts are generated the current day and the change compared with the last day.	10.0, 0.01%
New Alarm	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of new alerts the current day and the change compared with the last day.	10.0, -0.01%
Fix Alarm	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of handled alerts the current day and the change compared with the last day.	10.0, 0.01%

Widget	Display method	Default time range	Description	Example
High Level Alarm	Single value comparison	Today (Time Frame) and Compare with Yesterday	The number of critical alerts the current day and the change compared with the last day.	10.0, -0.01%
Alarm Operation Trend	Flow diagram	Today (Time Frame)	The trend in the number of operations on alerts, such as operations on new alerts and alert handling, per hour.	None
Alarm Level Trend	Flow diagram	Today (Time Frame)	The trend in the number of alerts at different priorities, such as critical, suspicious, and warning, per hour.	None
Alarm Status Trend	Flow diagram	Today (Time Frame)	The trend in the number of alerts in different states, such as unfixed and fixed, per hour.	None
Alarm Operation Distribution	Doughnut chart	Today (Time Frame)	The distribution of operations on alerts, such as operations on new alerts and alert handling.	None
Alarm Level Distribution	Doughnut chart	Today (Time Frame)	The distribution of alerts at different priorities, such as critical, suspicious, and warning.	None

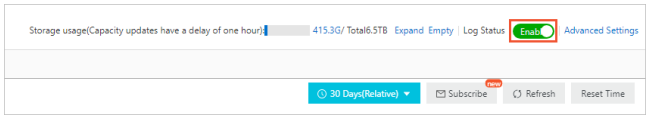
Widget	Display method	Default time range	Description	Example
Alarm Status Distribution	Doughnut chart	Today (Time Frame)	The distribution of the latest states of alerts, such as unfixed, fixed, and fix failed. **Notice** If an alert has multiple states, the latest state is used.	None
New Alarm Top10	Doughnut chart	Today (Time Frame)	Top 10 alerts that are generated the most on each host.	None
Fix Alarm Top10	Doughnut chart	Today (Time Frame)	Top 10 alerts that are handled the most on each host.	None
Alarm Client Distribution Top20	Table	Today (Time Frame)	Top 20 hosts for which the most alerts are generated. The table contains the following fields: Client, Alarm Event, New, Dealing, Serious, Suspicious, and Alarm Type.	None

1.7. View log reports

After you enable the log analysis feature, Security Center automatically provides **dashboards** and displays them on the **Log Reports** tab. You can perform the following operations on a dashboard: specify a time range, subscribe to log reports, refresh data, configure refresh settings, and view data in the dashboard. The data in the dashboard is updated based on your operations.

Prerequisites

Log Status in the right side of the **Log Analysis** tab is set to **Enabled**. If Log Status is set to Disabled, the system does not display log reports.



Context

On the **Log Reports** tab, you can view the following nine dashboards that are automatically provided.

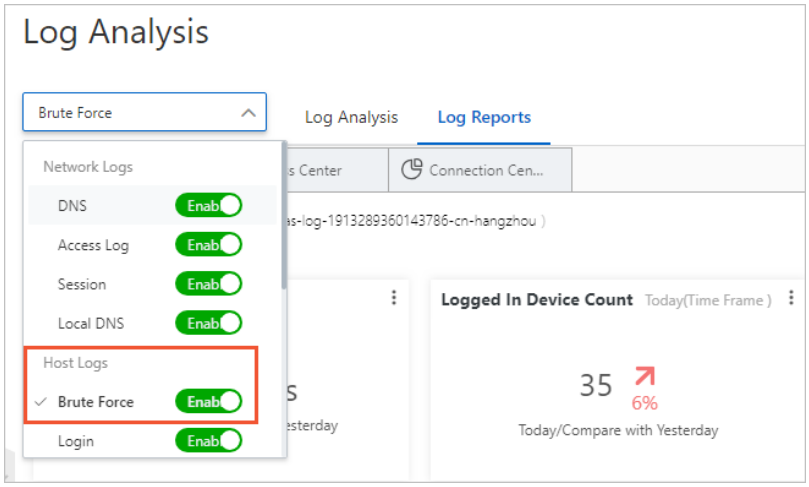
- Security
  - Alarm Center
  - Vulnerability Center
  - Baseline Center
- Host
  - Login Center
  - Process Center
  - Connection Center
- Network
  - DNS Access Center
  - Web Access Center
  - Network Session Center

For more information about the widgets in these dashboards, see Dashboards on the Log Reports tab.

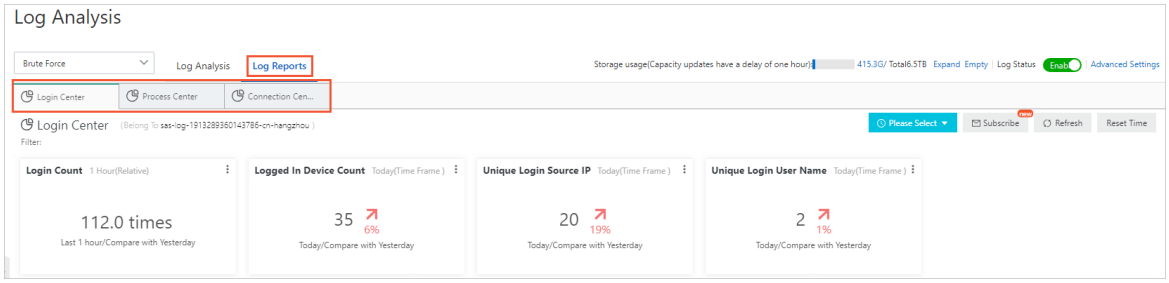
Procedure

To view log reports, perform the following steps:

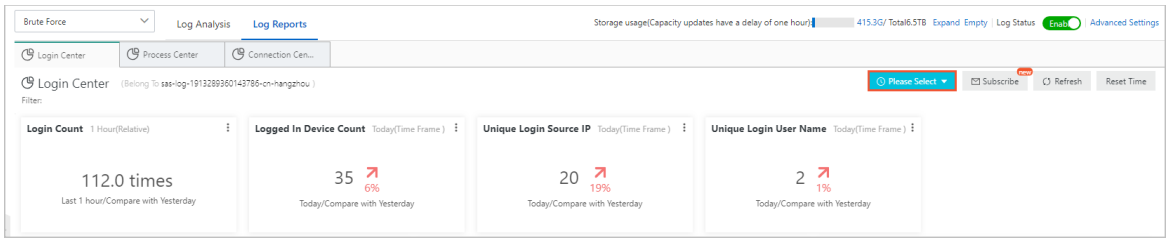
1. Log on to the Security Center console.
2. In the left-side navigation pane, choose **Investigation > Log Analysis**.
3. On the **Log Analysis** page, click the **Log Report** tab. Select a type of host log from the drop-down list. For example, select **Host Logs > Brute Force**. The Log Reports tab displays the sub-tabs for host log reports.



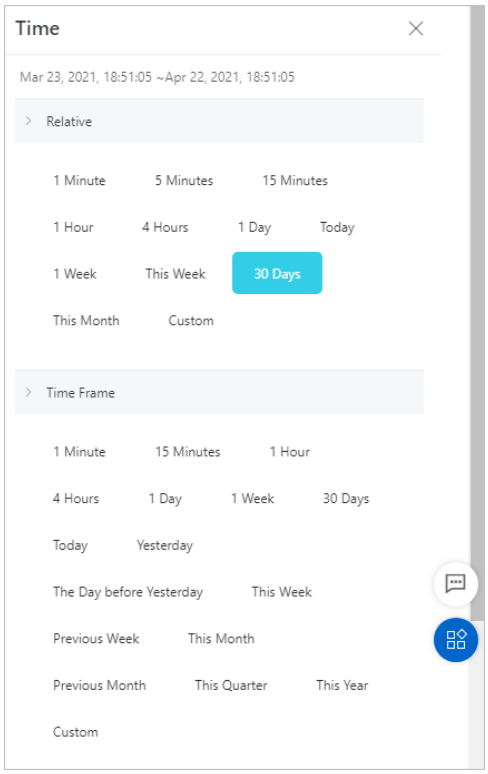
4. Click **Login Center**, **Process Center**, or **Connection Center**. The sub-tab for each type of log report appears.



5. Click **Please Select** in the upper-right corner of the **Login Center**, **Process Center**, or **Connection Center** sub-tab. The **Time** panel appears.



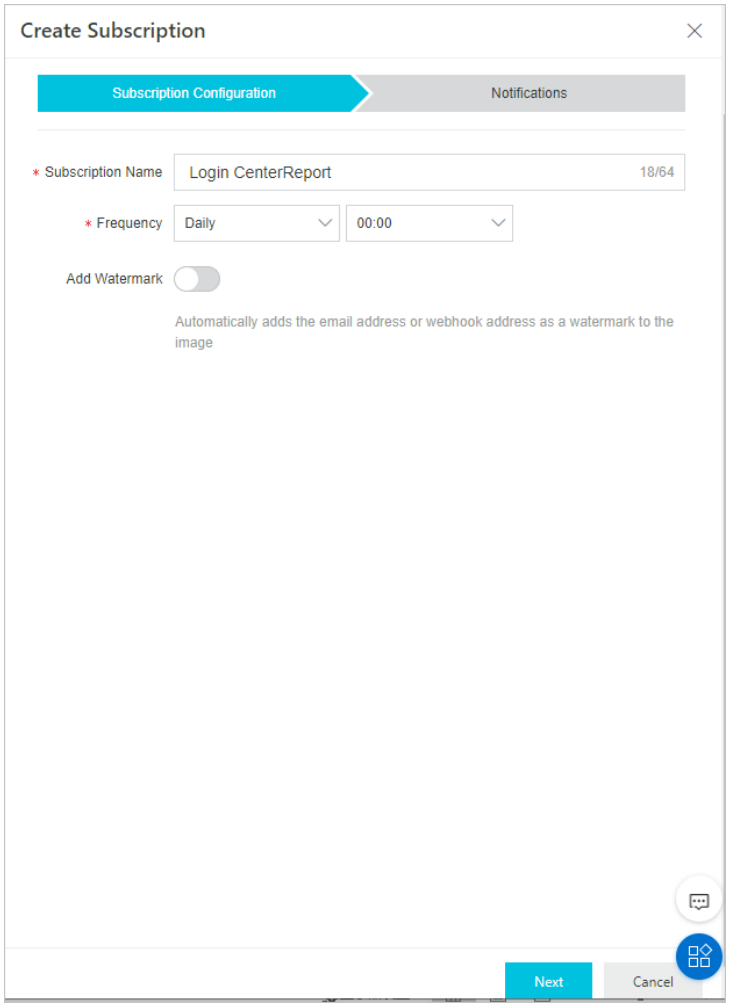
6. In the **Time** panel, specify a time range based on your business requirements and click **OK**. You can specify a time range in the Relative, Time Frame, or Custom sections.



Note

- After you specify a time range, the widgets on the dashboard display the data within the time range.
- The system applies the time setting only to the current sub-tab and does not save the settings. The next time you open this sub-tab, the dashboard displays data based on the default time setting.

7. Optional. Click **Subscribe** in the upper-right corner of the **Login Center**, **Process Center**, or **Connection Center** sub-tab. In the **Create Subscription** wizard, subscribe to the log report that corresponds to the sub-tab.
   i. In the **Subscription Configuration** step, configure the parameters such as Subscription Name and Frequency.

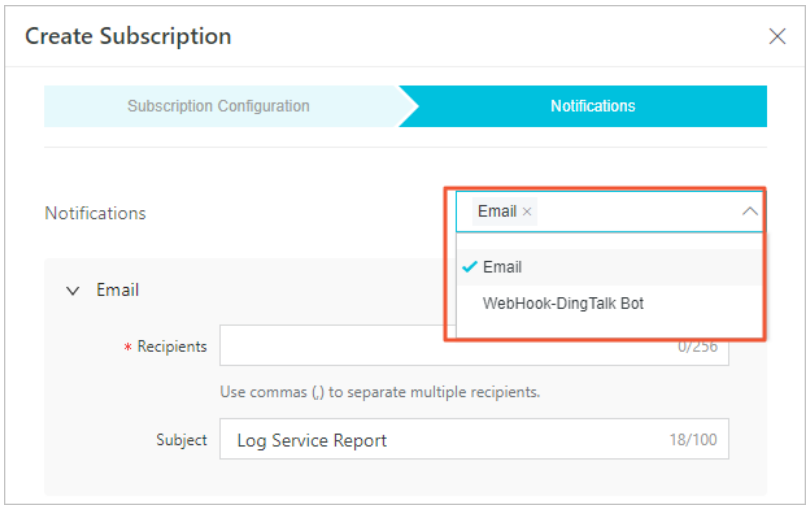


The following list describes the parameters:

- **Subscription Name**: the name of the log report to which you want to subscribe. The system automatically provides a name based on the type of log. You can replace the provided name with a custom one.

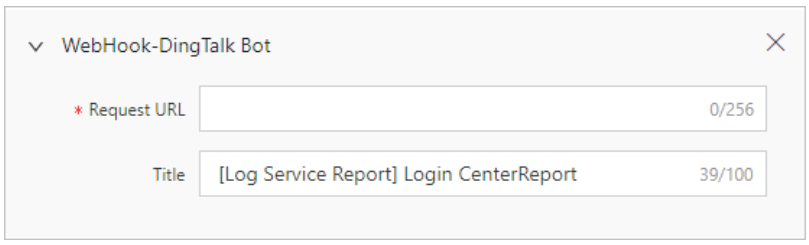
- **Frequency**: the frequency at which the system sends the subscribed log report.
  - **Hourly**: The system sends the log report every hour on the hour.
  - **Daily**: The system sends the log report every day at the same time. You can set the time to the exact beginning of an hour from 00:00 to 23:00.
  - **Weekly**: The system sends the log report every week at the same time. You can set the time to the exact beginning of an hour from 00:00 to 23:00 on **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
  - **Fixed Interval**: The system sends the log report at fixed intervals of days or hours.
  - **Cron**: The system sends the log report based on the cron expression that you enter. The time specified in the cron expression is accurate to minutes and is in the 24-hour notation. You can refer to the examples in the console to enter a cron expression.
- **Add Watermark**: If you turn on Add Watermark, the system adds your notification settings as watermarks to the images in the log report. The notification settings can be an email address or webhook request URL.

ii. Click **Next** to set the Notifications parameter.



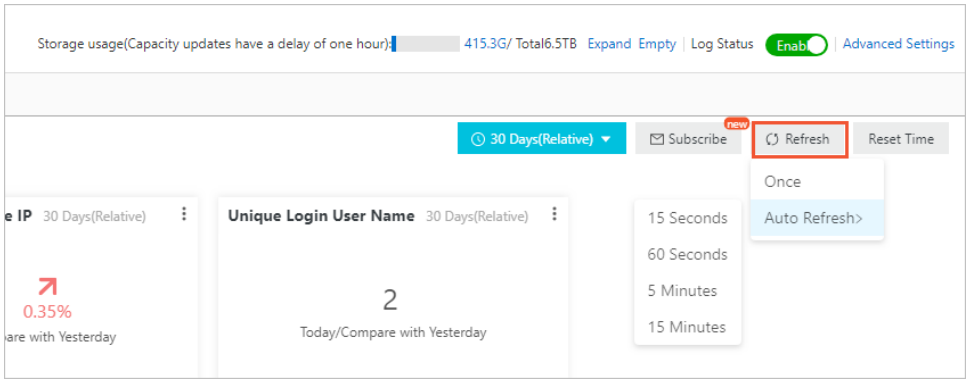
You can select one of the following notification methods:

- **Email**: Add the email address of a recipient. You can add more than one email address.
- **WebHook-DingTalk Bot**: Add a webhook request URL. For more information about how to obtain a webhook request URL, see Configure DingTalk chatbot notifications.



iii. Click **Submit**.

8. Optional. Click **Refresh** in the upper-right corner of the **Login Center**, **Process Center**, or **Connection Center** sub-tab. Then, configure the refresh settings for the log report.



You can use one of the following refresh settings:

- **Once**: The system immediately refreshes the log report.
- **Auto Refresh**:The system refreshes the log report at a specific time interval. Valid values: 15 Seconds, 60 Seconds, 5 Minutes, and 15 Minutes.

1.8. Export log data

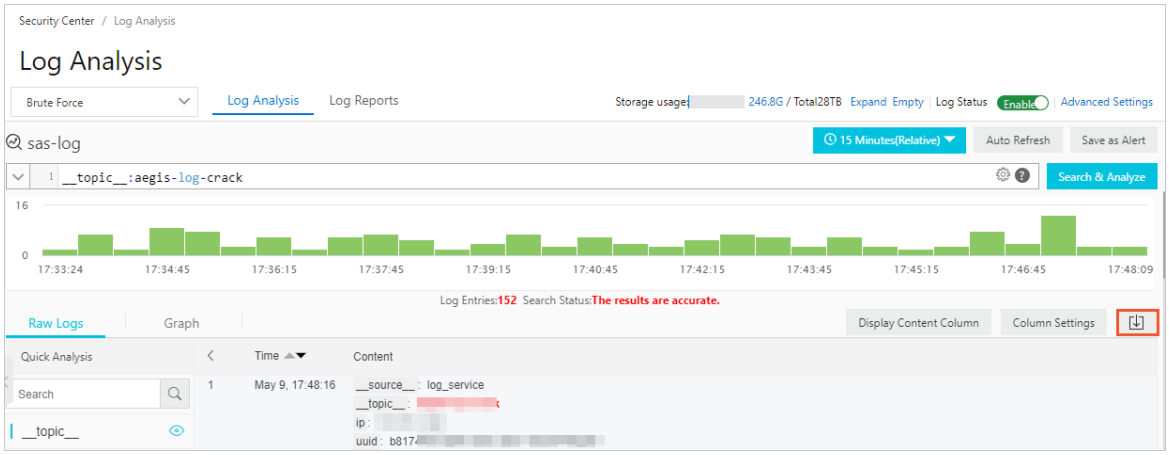
The log analysis feature of Security Center supports exporting log data to a local machine. You can download log data on a specified page to a local CSV file or all log data to a TXT file. This topic describes how to export log data.

Procedure

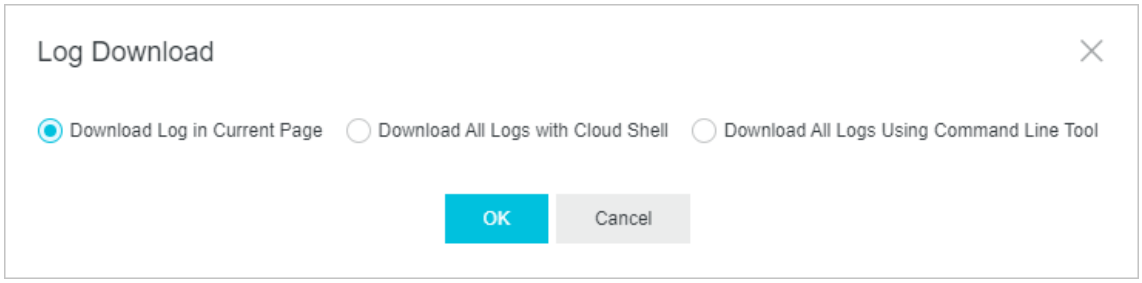
1. Log on to the Security center console.
2. In the left-side navigation pane, click **Investigation > Log Analysis**.
3. On the right of the **Raw Logs** tab, click

   to open the **Log Download** dialog box.

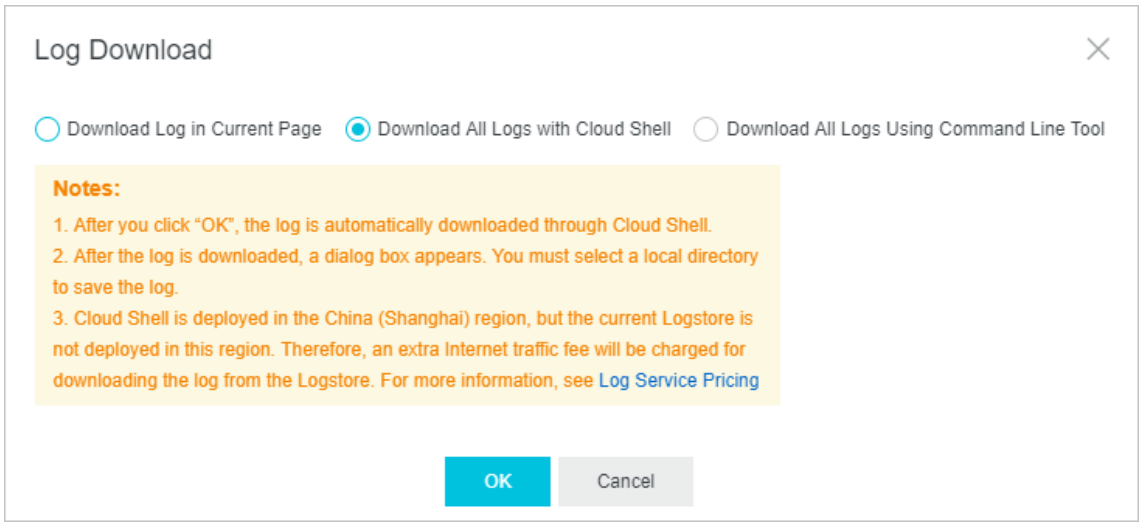


4. In the **Log Download** dialog box that appears, select a download method to export log data.
   - Select **Download Log in Current Page**, and click **OK**.



Log data on the specified page is exported to a local CSV file.

- Select **Download All Logs with Cloud Shell** to download all log data.

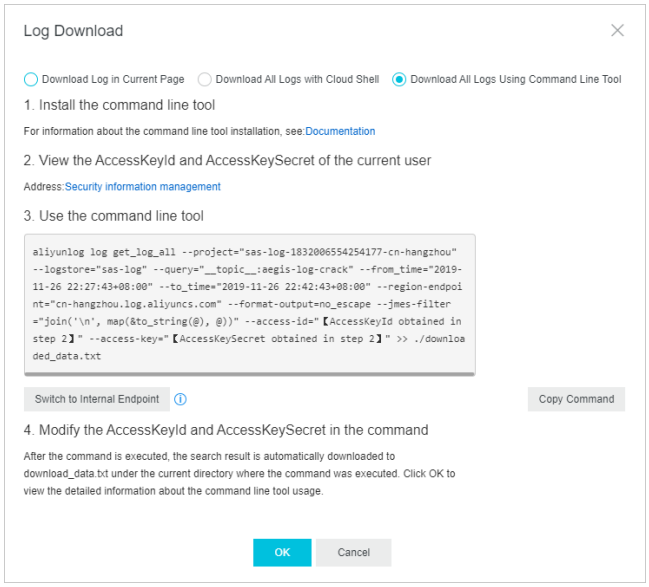


  a. Click **OK** to go to the **Cloud Shell** command line.
  b. Follow the instructions that appear on the page to enter the required information.
  c. Specify a local path where you want to store the log file.

All logs of Security Center are saved to a local TXT file.

> **Note** Currently, Cloud Shell is deployed in the China (Shanghai) region. If the current Logstore is not in the China (Shanghai) region, downloading log data incurs data consumption fees. Click **Log Service Pricing** to learn more about the pricing of data usage.

- Select **Download All Logs Using Command Line Tool** to download all log data.



a. Click **Documentation** in the Log Download dialog box to learn how to install a command line tool.

b. Install the command line tool.

c. Click **Security information management** to view and copy the AccessKey ID and AccessKey secret of the current user.

d. Click **Copy Command** and replace the `AccessKey ID in step 2` and `AccessKey secret in step 2` with those of the current user.

e. Run the command in the CLI command line tool.

After you run the command, all the log data of Security Center are automatically downloaded and saved to the **download_data.txt** file in the current directory where the command is executed.

1.9. Advanced settings

The log analysis feature provided by Security Center supports advanced settings. You can click Advanced Settings in the upper-right corner of the Log Analysis page to go to the Log Service console. In the Log Service console, you can perform advanced operations, such as configuring alerts and notifications, subscribing to log data, consuming log data, shipping data to other services, and visualizing data for other services.

Procedure

1.

2.

3. In the upper-right corner of the **Log Analysis** page, click **Advanced Settings**.

4. In the message that appears, click **Go** to go to the Log Service console.

5. In the Log Service console, perform operations based on your requirements.

   For more information about operations in the Log Service console, see the following topics:

   - Configure an alert rule
   - Configure notification methods
   - Data shipping

   > **Note** Log Service also allows you to call API operations to write log data to Log Service, search for log data, and manage projects and Logstores. For more information about the Log Service API, see Overview of the Log Service API.

2.FAQ

This topic provides answers to some frequently asked questions about the Investigation module of Security Center.

The collection of asset fingerprints is disabled. Why is the latest scan time updated?

In the **Settings** dialog box of a tab on the Asset Fingerprints page, all parameters are set to **Disable**. However, the value in the **Latest Collection Time** column of the tab is still updated. Why?

The latest scan time that is displayed in the **Latest Collection Time** column is updated on the tab because Log Service is activated. After you activate Log Service, Security Center collects the information about fingerprints of an asset for log analysis. Therefore, the latest scan time is updated on the tab.

No statistics are displayed on the Asset Fingerprints page. Why?

After you purchase the or edition of Security Center, Security Center does not automatically collect asset fingerprints. If you do not manually collect asset fingerprints, no statistics are displayed on the Asset Fingerprints page. To view statistics on the Asset Fingerprints page, you must configure scheduled collection tasks or manually collect asset fingerprints. For more information, see Collect asset fingerprints.