1 Security Log Auditing Commands

Command	Function
security-log audit-enable	Enable security log auditing.
security-log auto-vacuum-time	Configure the handling time of aged security logs.
security-log data-store-days	Configure the local storage time of security logs.
security-log data-store-items	Configure the local storage capacity for security logs.
security-log delete all	Clear logs for all key operations.
show security-log	Display all security logs.
show security-log config	Display security log configurations.
show security-log detail	Display detailed security log information.
show security-log detail export	Display detailed security log information.
show security-log detail stat	Display detailed security log statistics.
show security-log info	Display statistics during log processing.
show security-log statistics	Display security log statistics.

1.1 security-log audit-enable

Function

Run the **security-log audit-enable** command to enable security log auditing.

Run the **no** form of this command to disable this feature.

Security log auditing is enabled by default.

Syntax

security-log audit-enable

no security-log audit-enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

After the security log auditing function is enabled, the device records logs for key operations, including account management, login events, system events, configuration file changes, and auditing events.

Examples

The following example enables security log auditing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# security-log audit-enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 security-log auto-vacuum-time

Function

Run the **security-log auto-vacuum-time** command to configure the handling time of aged security logs.

The default handling time of aged security logs is **03:00:00** every day.

Syntax

security-log auto-vacuum-time *hh*:*mm*:*ss*

Parameter Description

hh:*mm*:*ss*: Handling time of aged security logs. Here, *hh* indicates the hour, *mm* indicates the minute, and *ss* indicates the second.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command is used to configure the time for checking local logs. By default, the system checks whether any local logs have exceeded the storage time at 03:00:00 every day and deletes expired logs.

Examples

The following example sets the handling time for aged security logs to 05:05:00 every day.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# security-log auto-vacuum-time 05:05:00
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 security-log data-store-days

Function

Run the **security-log data-store-days** command to configure the local storage time of security logs.

The default local storage time of security logs is **65535** days.

Syntax

security-log data-store-days *data-store-time*

Parameter Description

data-store-time: Local storage time of security logs, in days. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

- This command is used to configure the local storage time of security logs.
- The security logs for key operations are stored in the local database for **65535** days by default, and expired logs will be deleted.

Examples

The following example sets the local storage time of security logs to 300 days.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# security-log data-store-days 300
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 security-log data-store-items

Function

Run the **security-log data-store-items** command to configure the local storage capacity for security logs.

The maximum and minimum local storage capacity for security logs are **10000** and **500** (standard security requirements), respectively by default.

Syntax

security-log data-store-items *log-number*

Parameter Description

log-number: Local storage capacity for security logs. The value range is from 500 to 10000.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

If the local storage space is insufficient, you can run this command to decrease the storage capacity for security logs.

Examples

The following example sets the local storage capacity for security logs to 5000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# security-log data-store-items 5000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 security-log delete all

Function

Run the **security-log delete all** command to clear logs for all key operations.

Syntax

security-log delete all

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example clears logs for all key operations.

```
Hostname> enable
Hostname# security-log delete all
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.6 show security-log

Function

Run the **show security-log** command to display all security logs.

Syntax

show security-log

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays all security logs.

```
Hostname> enable
Hostname# show security-log
time, username, peerinfo, hostname, log-type: content
```

```
2019-01-01 10:00:02, -, console, Hostname, SEC_LOG: SECURITY_LOG enabled security
log audit configuration successfully
2019-01-01 10:00:02, admin, vty0(192.168.111.111), Hostname, SEC_LOG:
SECURITY_LOG disabled security log audit configuration unsuccessfully
2019-01-01 10:00:02, admin, vty0(192.168.111.111), Hostname, SEC_LOG:
SECURITY_LOG deleted all security log successfully
……
```

Table 1-1Output Fields of the show security-log Command

Field	Description
time	Log generation time
username	Username
peerinfo	Terminal information, including the terminal name, IP address, or both
hostname	Host name
log-type	Log type, including: ● SEC_LOG (security log events) ● ACC_MNT (account management) ● LOGIN (login events) ● SYS (system events) ● CONFIG (configuration file changes) ● OTHER (others)
content	Log content

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 show security-log config

Function

Run the **show security-log config** command to display security log configurations.

Syntax

show security-log config

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to display security log configurations, including whether log auditing is enabled, log capacity limit, log storage time, and handling time for aged security logs.

Examples

The following example displays security log configurations.

```
Hostname> enable
Hostname# show security-log config
Security-log audit: enable
Limit number: 10000
Store days: 180
Auto vacuum time: 03:00:00
Security-log send to syslog: enable
```

Table 1-1 Output Fields of the show security-log config Command

Field	Description
Security-log audit	Status of the security log auditing function: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Limit number	Security log capacity limit
Store days	Security log storage days
Auto vacuum time	Handling time of aged security logs
Security-log send to syslog	Status of the function of sending security logs to the syslog server

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 show security-log detail

Function

Run the **show security-log detail** command to display detailed security log information.

Syntax

show security-log detail { **all** | { **from** *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss* } } [**hostname** *hostname*] [**log-type** { **ACC_MNT** | **CONFIG** | **LOGIN** | **OTHER** | **SEC_LOG** | **SYS** }] [**peerinfo** *peerinfo*] [**user** *username*] { [**order-by** { **log-type** | **time** } { **asc** | **desc** } [**start-item** *start-item* **end-item** *end-item*]] }

Parameter Description

all: Displays all security logs.

from *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss*: Specifies the time range within which security logs are displayed. **from** specifies the start time, **to** specifies the end time, *YY* specifies the year, *MM* specifies the month, *DD* specifies the day, *hh* specifies the hour, *mm* specifies the minute, and *ss* specifies the second.

hostname *hostname*: Specifies the host name based on which security logs are displayed.

log-type: Specifies the log type based on which security logs are displayed. **SEC_LOG** specifies security log events, **ACC_MNT** specifies account management, **LOGIN** specifies login events, **SYS** specifies system events, **CONFIG** specifies configuration file changes, and **OTHER** specifies others.

peerinfo *peerinfo*: Specifies the terminal information based on which security logs are displayed. The terminal information can be the terminal name, terminal IP address, or both, such as vty0 (192.168.1.1).

user *username*: Specifies the user name based on which security logs are displayed.

order-by log-type: Orders logs by log type.

order-by time: Orders logs by log time.

asc: Orders logs in ascending mode.

desc: Orders logs in descending mode.

start-item *start-item*: Specifies the start position in the search result. The value range is from 1 to 10000.

end-item *end-item*: Specifies the end position in the search result. The value range is from 1 to 10000.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to display detailed security log information, which can be filtered by time, log type, username, host name, and terminal information.

Examples

The following example displays all security logs.

```
Hostname> enable
Hostname# show security-log detail all
time, username, peerinfo, hostname, log-type: content
2019-10-22 10:00:02, admin, vty0(192.168.111.111), Hostname, SEC_LOG:
SECURITY_LOG deleted all security log successfully
2019-10-22 10:00:02, admin, vty0(192.168.111.111), Hostname, SEC_LOG:
SECURITY_LOG disabled security log audit configuration unsuccessfully
2019-10-22 10:00:03, -, console, Hostname, SEC_LOG: SECURITY_LOG enabled security
log audit configuration successfully
……
```

Table 1-1Output Fields of the show security-log detail all Command

Field	Description
time	Log generation time
username	Username
peerinfo	Terminal information, including the terminal name, IP address, or both
hostname	Host name
log-type	Log type, including: ● SEC_LOG (security log events) ● ACC_MNT (account management) ● LOGIN (login events) ● SYS (system events) ● CONFIG (configuration file changes) ● OTHER (others)
content	Log content

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 show security-log detail export

Function

Run the **show security-log detail export** command to display detailed security log information.

Syntax

show security-log detail export { **all** | { **from** *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss* } } [**hostname** *hostname*] [**log-type** { **ACC_MNT** | **CONFIG** | **LOGIN** | **OTHER** | **SEC_LOG** | **SYS** }] [**peerinfo** *peerinfo*] [**user** *username*] { [**order-by** { **log-type** | **time** } { **asc** | **desc** } [**start-item** *start-item* **end-item** *end-item*]] }

Parameter Description

all: Exports all security logs.

from *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss*: Specifies the time range within which security logs are exported. **from** specifies the start time, **to** specifies the end time, *YY* specifies the year, *MM* specifies the month, *DD* specifies the day, *hh* specifies the hour, *mm* specifies the minute, and *ss* specifies the second.

hostname *hostname*: Specifies the host name based on which security logs are exported.

log-type: Specifies the log type based on which security logs are exported. **SEC_LOG** specifies security log events, **ACC_MNT** specifies account management, **LOGIN** specifies login events, **SYS** specifies system events, **CONFIG** specifies configuration file changes, and **OTHER** specifies others.

peerinfo *peerinfo*: Specifies the terminal information based on which security logs are exported. The terminal information can be the terminal name, terminal IP address, or both, such as vty0 (192.168.1.1).

user *username*: Specifies the user name based on which security logs are exported.

order-by log-type: Orders logs by log type.

order-by time: Orders logs by log time.

asc: Orders logs in ascending mode.

desc: Orders logs in descending mode.

start-item *start-item*: Specifies the start position in the export result. The value range is from 1 to 10000.

end-item *end-item*: Specifies the end position in the export result. The value range is from 1 to 10000.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to export detailed security log information, which can be filtered by time, log type, username, host name, and terminal information.

You can run the **copy** command to download the exported file. The following shows an example.

```
Hostname# copy tmp:mng/security_log/export_file/log_20191022_110410_535250.csv
tftp://192.168.1.1/security_log.csv
```

Examples

The following example exports security logs of user A during the time range from 00:00:00 October 10, 2019 to 24:00:00 October 22, 2019.

```
Hostname> enable
Hostname# show security-log detail export from 2019 10 10 00:00:00 to 2019 10 22
23:59:59 user userA
Export file: tmp:mng/security_log/export_file/log_20191022_110410_535250.csv
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 show security-log detail stat

Function

Run the **show security-log detail stat** command to display detailed security log statistics.

Syntax

show security-log detail stat { **all** | { **from** *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss* } } [**hostname** *hostname*] [**log-type** { **ACC_MNT** | **CONFIG** | **LOGIN** | **OTHER** | **SEC_LOG** | **SYS** }] [**peerinfo** *peerinfo*] [**user** *username*]

Parameter Description

all: Displays all security logs.

from *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss*: Specifies the time range within which security logs are displayed. **from** specifies the start time, **to** specifies the end time, *YY* specifies the year, *MM* specifies the month, *DD* specifies the day, *hh* specifies the hour, *mm* specifies the minute, and *ss* specifies the second.

hostname *hostname*: Specifies the host name based on which security logs are displayed.

log-type: Specifies the log type based on which security logs are displayed. **SEC_LOG** specifies security log events, **ACC_MNT** specifies account management, **LOGIN** specifies login events, **SYS** specifies system events, **CONFIG** specifies configuration file changes, and **OTHER** specifies others.

peerinfo *peerinfo*: Specifies the terminal information based on which security logs are displayed. The terminal information can be the terminal name, terminal IP address, or both, such as vty0 (192.168.1.1).

user *username*: Specifies the user name based on which security logs are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to display detailed security log statistics, which can be filtered by time, log type, username, host name, and terminal information.

Examples

The following example displays security log statistics of user A during the time range from 00:00:00 October 10, 2019 to 24:00:00 October 22, 2019.

```
Hostname# show security-log detail stat from 2019 10 10 00:00:00 to 2019 10 22
23:59:59 user userA
Count:555
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show security-log info

Function

Run the **show security-log info** command to display statistics during log processing.

Syntax

show security-log info

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

N/A

Examples

The following example displays security log statistics.

```
Hostname> enable
Hostname# show security-log info
Receive log count: 2000, err 1
Send syslog count: 1800
Current cached record count: 1999
Current store-in-flash record count: 5000
Historital sync flash count: 100, err 1
Reason for last sync failure: Failed to sync security logs to file database.
Next time to sync flash: 11:11:11
```

Table 1-1Output Fields of the show security-log info Command

Field	Description
Receive log count	Number of successfully received logs (xxx) and number of logs failed to be received (xxx)
Current cached record count	Number of cached logs
Current store-in-flashrecord count	Number of logs stored in the flash memory
Historital sync flash count	Number of historical synchronization times to the flash memory (xxx) and number of failed synchronizations (xxx)
Reason for last sync failure	Reason for the last synchronization failure (which is displayed if a synchronization failure occurred and not displayed if no synchronization failure occurs)
Next time to sync flash	Next synchronization time to the flash memory, in HH:MM:SS format

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 show security-log statistics

Function

Run the **show security-log statistics** command to display security log statistics.

Syntax

show security-log statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to display security log statistics, including the number of recorded logs and last deleted log. For details, see Table 1-1.

Examples

The following example displays security log statistics.

```
Hostname> enable
Hostname# show security-log statistics
Current storage record count: 9000
Historical record count: have written 11111, overwritten 1111
Aging record count: 1000
Last delete record: 2019-10-24 10:00:00 userA vty0(192.168.1.1) Hostname SEC_LOG:
SECURITY_LOG deleted all security log successfully
```

Table 1-1 Output Fields of the show security-log statistics Command

Field	Description
Current cache record count	Number of cached logs
Current storage record count	Number of locally stored logs
Historical storage record count	Number of historically stored logs in the local database, including the total number of stored logs (xxx) and the number of overwritten logs (xxx)
Aging record count	Number of aged logs in the local database
Last delete record	Last deleted log

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A