Contents

1 Configuring Security Log Auditing

1.1 Introduction

1.1.1 Overview

Security log auditing is used to record key operations on a device and audit and backtrack these operations afterwards to improve the device security and meet the national security standards.

Instruction

The following sections describe content related to security log auditing only.

1.1.2 Principles

1. Basic Concepts

- Key operation

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

  - Adding/deleting accounts
  - Editing authentication information
  - Modifying configurations (such as the DNS address and IP address)
  - User login/logout
  - Restarting/Stopping the device
  - Uploading/downloading files (when supported)
  - Editing user permissions (when supported)
  - Enabling/disabling log auditing and deleting logs

2. Enabling Security Log Auditing

After the security log auditing function is enabled, the device can record logs for key operations and locally store the logs.

When a user performs a key operation, such as account management, login/logout, system restart, configuration file change, or log auditing function enabling/disabling, the corresponding service module will collect information (such as time, username, IP address, operation log content, and operation result), generate a log, and write the log to the local database through the log auditing framework.

At 03:00:00 a.m. each day, the system checks whether any logs for key operations exceed the storage time. If yes, the logs will be deleted.

A maximum of 10,000 logs can be stored by default. After the number of stored logs exceeds the storage limit, new logs will overwrite the earliest ones.

3. Enabling the Function of Sending Security Logs to the Syslog Server

After a device is configured with the functions of syslog, and the security log auditing and sending functions are enabled, the log auditing framework will send generated logs to the syslog server to store.

1.2 Restrictions and Guidelines

- To protect the flash storage chip, newly generated logs will be cached in the memory and written to a file every 1 hour. When a restart command, such as **reload**, is executed, logs will be written to a file. If many logs are generated in this hour and some logs are not written to the file in 1 hour, the logs will be lost.
- When logs are exported to a file, download the file in time. The file will be automatically deleted after 1 hour.

1.3 Configuration Task Summary

Configuration of security log auditing includes the following tasks:

(1)Enabling Security Log Auditing

(2)(Optional) Configuring the Local Storage Time for Security Logs

(3)(Optional) Configuring the Handling Time of Aged Security Logs

(4)(Optional) Configuring the Local Storage Capacity for Security Logs

(5)Ошибка: источник перекрёстной ссылки не найден

1.4 Configuring Security Log Auditing

1.4.1 Overview

The security log auditing function can record logs for key operations on a device and locally store the logs. Log query and export are supported.

1.4.2 Enabling Security Log Auditing

1. Overview

After the security log auditing function is enabled, the device will record logs for key operations, including account management, login events, system events, configuration file changes and security log events, and store the logs to the local database.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable security log auditing.

security-log audit-enable

Security log auditing is enabled by default.

1.4.3 Configuring the Local Storage Time for Security Logs

1. Overview

After the local storage time is configured for security logs, the logs that have exceeded the storage time will be deleted.

2. Restrictions and Guidelines

Security logs that have exceeded the storage time will be deleted.

3. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the local storage time for security logs.

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

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

1.4.4 Configuring the Handling Time of Aged Security Logs

1. Overview

After the handling time of aged security logs is configured, the system checks whether any logs have exceeded the storage time at the configured handling time (deviation: 5 minutes) and deletes expired logs.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the handling time of aged security logs.

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

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

1.4.5 Configuring the Local Storage Capacity for Security Logs

1. Overview

After the local storage capacity for security logs is configured, new logs will overwrite earliest ones when the capacity of locally stored logs exceeds the storage limit.

2. Restrictions and Guidelines

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

3. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the local storage capacity for security logs.

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

The default local storage capacity for security logs is **10000**.

1.5 Monitoring

Run the **delete** commands to clear information.

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** commands to output debugging information.

Notice

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1Monitoring

Command	Purpose
debug security-log errors	Debugs log auditing.
debug security-log recv-info	Debugs received logs.
debug security-log sql-info	Debugs the log database.
show security-log	Displays all logs.
show security-log config	Displays configurations.
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*]] }	Displays the detailed log information, which can be filtered by time, log type, username, host name, and terminal information.
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-**	Exports the detailed log information, which can be filtered by time, log type, username, host name, and terminal information.

Command	Purpose
item *end-item*]] }	
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*]	Displays the log statistics, which can be filtered by time, log type, username, host name, and terminal information.
show security-log info	Displays the statistics during log processing.
show security-log statistics	Displays the statistics.
security-log delete all	Deletes all logs.

1.6 Configuration Examples

1.6.1 Configuring Security Log Auditing

1. Requirements

To improve device security and audit and backtrack exceptions (such as key configurations being tampered) afterwards, key operations on a device need to be recorded. After the security log auditing function is enabled, the device records key operations, including account management, login events, system events, configuration file changes, and security log events. After logging in to the device, the administrator can monitor recent user behaviors through the records.

2. Topology

Figure 1-1Configuring Security Log Auditing

PC Device

3. Notes

- Enable security log auditing.
- Configure parameters related to security log auditing.

4. Procedure

Enable security log auditing.

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

Set the local storage time of security logs to **300** days.

```
Device(config)# security-log data-store-days 300
```

Set the handling time of aged security logs to **05:05:00** every day.

```
Device(config)# security-log auto-vacuum-time 05:05:00
```

Set the local storage capacity for security logs to **1000**.

```
Device(config)# security-log data-store-items 1000
```

5. Verification

Log in to the device, perform key operations, and run **show security-log detail all** 30s later to check the log auditing records.

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

Run the **show security-log config** command to verify that the local storage time of security logs is 300 days, the handling time of aged security logs is 05:05:00 every day, and the local storage capacity for security logs is 1000.

```
Device# show security-log config
Security-log audit: enable
Limit number: 10000
Store days: 300
Auto vacuum time: 05:05:00
```

6. Configuration Files

Device configuration file

```
hostname Device
!
security-log data-store-days 300
security-log data-store-items 1000
security-log auto-vacuum-time 05:05:00
!
end
```