Implementing System Logging

This module describes the tasks you need to implement logging services on the router.

The Cisco IOS XR Software provides basic logging services. Logging services provide a means to gather logging information for monitoring and troubleshooting, to select the type of logging information captured, and to specify the destinations of captured system logging (syslog) messages.

Feature History for Implementing System Logging

Release	Modification
Release 6.1.2	Platform Automated Monitoring (PAM) tool was introduced for all Cisco IOS XR 64-bit platforms.

Implementing System Logging

System Logging (Syslog) is the standard application used for sending system log messages. Log messages indicates the health of the device and point to any encountered problems or simplify notification messages according to the severity level. The IOS XR router sends its syslog messages to a syslog process. By default, syslog messages will be sent to the console terminal. But, syslog messages can be send to destinations other than the console such as the logging buffer, syslog servers, and terminal lines.

Syslog Message Format

By default, the general format of syslog messages generated by the syslog process on the Cisco IOS XR software is as follows:

```
node-id : timestamp : process-name [pid] : % message category -group -severity -message
-code : message-text
```

The following table describes the general format of syslog messages on Cisco IOS XR software.

Table 1: Format of Syslog Messages

Field	Description
node-id	Node from which the syslog message originated.

Field	Description
timestamp	Time stamp in the month day HH:MM:SS format, indicating when the message was generated. **Note** The time-stamp format can be modified using the **service timestamps** command.
process-name	Process that generated the syslog message.
size	Process ID (pid) of the process that generated the syslog message.
[pid]	Message category, group name, severity, and message code associated with the syslog message.
message-text	Text string describing the syslog message.

Syslog Message Severity Levels

In the case of logging destinations such as console terminal, syslog servers and terminal lines, you can limit the number of messages sent to a logging destination by specifying the severity level of syslog messages. However, for the logging buffer destination, syslog messages of all severity will be sent to it irrespective of the specified severity level. In this case, the severity level only limits the syslog messages displayed in the output of the command **show logging**, at or below specified value. The following table lists the severity level keywords that can be supplied for the severity argument and the corresponding UNIX syslog definitions in order from the most severe level to the least severe level.

Note Utility word count lines are used to calculate the number of logs present in the IOS XR syslog buffer. When there is an increase in the inflow of logs from the routers, if you are executing the **show logging** command, the number of lines calculated by using the word count utility may exceed the value set for login buffer size. You can set the login buffer size by using the **logging buffer entries-count** command.

Table 2: Syslog Message Severity Levels

Severity Keyword	Level	Description
emergencies	0	System unusable
alert	1	Immediate action needed
critical	2	Critical conditions
errors	3	Error conditions
warnings	4	Warning conditions
notifications	5	Normal but significant condition
informational	6	Informational messages only

Severity Keyword	Level	Description
debugging	7	Debugging messages

Configuring Syslog Severity Level for Telemetry

The severity of syslog messages that are generated by the router varies from emergencies to simple notifications. You can specify a severity keyword corresponding to any one of the severity levels—from the highest severity level 0 (emergencies) through the lowest severity level 7 (debugging). Depending upon the severity level you have specified, the router streams data to the telemetry server, starting from the chosen severity level and higher.

You can specify the severity level by using the **logging yang** *severity-level* command.

Tip You can programmatically monitor syslog messages by using the `openconfig-messages.yang` OpenConfig data model. To get started with using data models, see the *Programmability Configuration Guide for Cisco NCS 5500 Series Routers*.

Configuration Example

This example sets **warnings** as the severity level. This results in the streaming of syslogs only for **warnings**, **errors**, **critical**, **alert**, and **emergencies**. Syslogs of lower severity are not streamed.

```
Router(config)#logging yang warnings
```

Telemetry Output

This example shows sample telemetry operational output when **logging yang warnings** command is configured.

```
--------
{"node_id_str":"ios","subscription_id_str":"app_TEST_200000001","encoding_path":
"openconfig-system:system","collection_id":"40","collection_start_time":"1664513125273",
"msg_timestamp":"1664513125273","data_json":[{"timestamp":"1664513125272","content":
{"messages":
{"state":{"severity":"EMERGENCY","message":
{"msg":"RP/0/0/CPU0:Sep 30 10:15:25.272 IST: logger[67820]: %OS-SYSLOG-0-LOG_EMERG :
TEST_EMERG ","priority":184,"app-name":"logger","procid":"67820","msgid":
"OS-SYSLOG-0-LOG_EMERG"}}}}}],"collection_end_time":"1664513125273"}
--------
 Sub_id 200000001, flag 4, len 534
--------
{"node_id_str":"ios","subscription_id_str":"app_TEST_200000001","encoding_path":
"openconfig-system:system","collection_id":"41","collection_start_time":"1664513137884",
"msg_timestamp":"1664513137884","data_json":[{"timestamp":"1664513137883","content":
{"messages":
{"state":{"severity":"WARNING","message":
{"msg":"RP/0/0/CPU0:Sep 30 10:15:37.882 IST: logger[67997]:
%OS-SYSLOG-4-LOG_WARNING : TEST_WARN
 ","priority":188,"app-name":"logger","procid":"67997","msgid":
"OS-SYSLOG-4-LOG_WARNING"}}}}}],"collection_end_time":"1664513137884"}
--------
 Sub_id 200000001, flag 4, len 529
--------
{"node_id_str":"ios","subscription_id_str":"app_TEST_200000001","encoding_path":
"openconfig-system:system","collection_id":"42","collection_start_time":
```

"1664513562626","msg_timestamp":"1664513562626","data_json":[{"timestamp":"1664513562624",
"content":{"messages":{"state":{"severity":"**CRITICAL**","message":
{"msg":"RP/0/0/CPU0:Sep 30 10:22:42.624 IST: logger[68957]: %OS-SYSLOG-2-LOG_CRIT :
TEST_CRIT ","priority":186,"app-name":"logger","procid":"68957","msgid":
"OS-SYSLOG-2-LOG_CRIT"}}}}}],"collection_end_time":"1664513562626"}

Sub_id 200000001, flag 4, len 529

{"node_id_str":"ios","subscription_id_str":"app_TEST_200000001","encoding_path":
"openconfig-system:system","collection_id":"43","collection_start_time":
"1664513570004","msg_timestamp":"1664513570004","data_json":[{"timestamp":"1664513570003",
"content":{"messages":{"state":{"severity":"**ALERT**","message":
{"msg":"RP/0/0/CPU0:Sep 30 10:22:50.002 IST: logger[69113]: %OS-SYSLOG-1-LOG_ALERT :
TEST_ALERT ","priority":185,"app-name":"logger","procid":"69113",
"msgid":"OS-SYSLOG-1-LOG_ALERT"}}}}}],"collection_end_time":"1664513570004"}

Sub_id 200000001, flag 4, len 525

{"node_id_str":"ios","subscription_id_str":"app_TEST_200000001","encoding_path":
"openconfig-system:system","collection_id":"44","collection_start_time":
"1664513844428","msg_timestamp":"1664513844428","data_json":[{"timestamp":"1664513844427","content":
{"messages":{"state":{"severity":"**ERROR**","message":
{"msg":"RP/0/0/CPU0:Sep 30 10:27:24.426 IST: logger[69203]: %OS-SYSLOG-3-LOG_ERR :
TEST_ERROR ","priority":187,"app-name":"logger","procid":"69203","msgid":
"OS-SYSLOG-3-LOG_ERR"}}}}}],"collection_end_time":"1664513844428"}

Bias-Free Terminology in Syslogs

Table 3: Feature History Table

Feature Name	Release Information	Feature Description
Bias-Free Terminology in Syslogs	Release 7.6.1	As part of ongoing efforts to use inclusive language in the IOS XR software and documentation, Cisco has created the **service cli neutral enable** command. When you execute this command, biased terms found in the logs of certain features are replaced with bias-free terms. There are certain other features that are not controlled by the command. The biased terms in these features are automatically replaced with bias-free terms. Cisco expects to convert these features to be controlled by the command in subsequent releases.

You have various features deployed in your network. The feature-specific log that you retrieve from the syslog server may contain biased terms. As part of the ongoing efforts to remove such biased terms, Cisco has introduced the **service cli neutral enable** command. Use this command to replace biased terms with bias-free terms in the logs of certain features. There are certain other features that automatically reflect these changes, and Cisco expects to convert these features to be controlled by the CLI in subsequent releases.

This table lists the features for which Cisco has automatically replaced biased terms. The table also lists the replaced, bias-free term.

Existing Log Information	Modified Log Information
WARN_TRAFFIC_**SLAVE**	WARN_TRAFFIC_**SUBORDINATE**
VRRP control packet received from %s on MGO **slave**: %s VRID %u	VRRP control packet received from %s on MGO **subordinate**: %s VRID %u
Type6 **masterkey** update still in progress. masterkey get failed	Type6 **key** update still in progress. Type6 key get failed.
Mastered get failed because of Type6 **masterkey** update still in progress.	Type6 **keys get** failed because of Type6 key update still in progress.
Received **master key** update event. Migrating existing type6 passwords. Database will be updated.	Received type6 **key** update event. Migrating existing type6 passwords. Database will be updated.
Completed migration of existing type6 passwords using the new **masterkey**. Database successfully updated.	Completed migration of existing type6 passwords using the new type6 **key**. Database successfully updated.
Decryption failed for keychain %s, keyid %s type6 password. Failed to migrate type6 keychains with the new **masterkey**	Decryption failed for keychain %s, keyid %s type6 password. Failed to migrate type6 keychains with the new type6 **key**
Keychain failed to process the **masterkey** update abort event from type6, err : %s	Keychain failed to process the type6 **key** update abort event from type6, err : %s
Type6 **masterkey** update : %s	Type6 **key** update : %s
Type6 **masterkey** %s successfully	Type6 **key** %s successfully
Type6 **masterkey** %s timeout	Type6 **key** %s timeout
Type6 **masterkey** %s successfully	Type6 **key** %s successfully
Type6 **masterkey** %s failed with Error: %s	Type6 **key** %s failed with Error: %s
All clients have not completed the **masterkey** abort operation. Forcing the abort operation.	All clients have not completed the type6 **key** update abort operation. Forcing the abort operation.
Type6 **masterkey** reconfig is inprogress. Unregister of client isn't allowed.	Type6 **key** reconfig is inprogress. Unregister of client is not allowed.
MASTERKEY_UPDATE	**MK**_UPDATE
WARN_TRAFFIC_**SLAVE**	WARN_TRAFFIC_**SUBORDINATE**
HSRP control packet received from %s on MGO **slave** group: %s group %u	HSRP control packet received from %s on MGO **subordinate** group: %s group %u

Existing Log Information	Modified Log Information
ROLE_**MASTER**	ROLE_ **PRIMARY**
ROLE_**SLAVE**	ROLE_**BACKUP**
Message: SYNC_DONE "please check if the affected sessions have been flagged as failed and these would be retried on the **Slave** side."	Message: SYNC_DONE "please check if the affected sessions have been flagged as failed and these would be retried on the **Backup** side."
SLAVE_UPD_FAIL	**BACKUP**_UPD_FAIL

This table lists the features for which you can run the **service cli neutral enable** command to change the biased terms.

Existing Log Information	Modified Log Information
ROLE_**MASTER**	"ROLE_**PRIMARY**"
ROLE_**SLAVE**	"ROLE_**BACKUP**"
SLAVE_UPD_FAIL	"**BACKUP**_UPD_FAIL"

Enable Bias-Free Configuration

Configuration Example

To replace biased terms with bias-free terms in your logs, run the following command:

```
RP/0/RP0/CPU0:router(config)#service cli neutral enable
RP/0/RP0/CPU0:router(config)#commit
Tue Mar 15 08:11:10.253 UTC
RP/0/RP0/CPU0:router(config)#end
```

If required, use the **no** form of the command to recall biased terms in your logs.

Verification

To verify that biased terms are replaced, run the following command

```
RP/0/RP0/CPU0:router#show running-config service cli neutral enable
Tue Mar 15 08:11:21.893 UTC
service cli neutral enable
```

This codeblock shows a sample output when the CLI is enabled:

```
RP/0/0/CPU0:Apr 13 12:01:04.371 IST: serg_agt[1188]: %INFRA-SERG-5-ROLE_PRIMARY : Session
Redundancy role change to Primary from Backup for group 2 reason ADMIN
LC/0/1/CPU0:Apr 13 12:01:04.372 IST: serg_agt[323]: %INFRA-SERG-5-ROLE_BACKUP : Session
Redundancy role change to Backup from Primary for group 1 reason ADMIN
RP/0/0/CPU0:Apr 13 12:01:04.377 IST: serg_agt[1188]: %INFRA-SERG-5-ROLE_BACKUP : Session
Redundancy role change to Backup from Primary for group 2 reason ADMIN
LC/0/1/CPU0:Apr 13 12:01:04.377 IST: serg_agt[323]: %INFRA-SERG-5-ROLE_PRIMARY : Session
Redundancy role change to Primary from Backup for group 1 reason ADMIN
```

This codeblock shows a sample output when the CLI is not enabled:

```
RP/0/0/CPU0:Apr 13 11:50:03.333 IST: serg_agt[1188]: %INFRA-SERG-5-ROLE_SLAVE : Session
Redundancy role change to Slave from None for group 2 reason PEER-UP
```

```
LC/0/1/CPU0:Apr 13 11:50:03.334 IST: serg_agt[323]: %INFRA-SERG-5-ROLE_MASTER : Session
Redundancy role change to Master from None for group 1 reason PEER-UP
RP/0/0/CPU0:Apr 13 11:50:03.338 IST: serg_agt[1188]: %INFRA-SERG-5-ROLE_MASTER : Session
Redundancy role change to Master from None for group 2 reason PEER-UP
LC/0/1/CPU0:Apr 13 11:50:03.339 IST: serg_agt[323]: %INFRA-SERG-5-ROLE_SLAVE : Session
Redundancy role change to Slave from None for group 1 reason PEER-UP
```

Prerequisites for Configuring System Logging

These prerequisites are required to configure the logging of system messages in your network operating center (NOC):

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- You must have connectivity with syslog servers to configure syslog server hosts as the recipients for syslog messages.

Configuring System Logging

Perform the tasks in this section for configuring system logging as required.

Configuring Logging to the Logging Buffer

Syslog messages can be sent to multiple destinations including an internal circular buffer known as logging buffer. You can send syslog messages to the logging buffer using the **logging buffered** command.

Configuration Example

This example shows the configuration for sending syslog messages to the logging buffer. The size of the logging buffer is configured as 3000000 bytes. The default value for the size of the logging buffer is 2097152 bytes.

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# logging buffered 3000000
RP/0/RP0/CPU0:Router(config)# commit
```

System Logging Message Count

Table 4: Feature History Table

Feature Name	Release Information	Feature Description
System Logging Message Count	Release 7.11.1	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) Instead of calculating the bytes consumed by Syslog as you did previously, you can now easily and effectively manage the buffer size of the system log messages by specifying the number of entries the system log displays. The feature introduces these changes: **CLI:** • The **entries-count** keyword is added to the **logging buffered** command. **YANG Data Model:** • New Xpaths for Cisco-IOS-XR-infra-syslog-cfg • New Xpaths for Cisco-IOS-XR-um-logging-cfg

Earlier, you were only able to configure the buffer size of the system log messages in bytes using the **logging buffered** command.

Starting Cisco IOS XR Software Release 7.11.1, you can you can specify the number of entries to be present while displaying the system logs. Based on the number of entries, the system internally calculates the buffer size and reserves the same for system log buffer. The default value is 2545. The range for sytem logging message count entry is from 2545 to 151699. When you disable the command, the logging buffer size points back to the default value of 2545.

If both the **logging buffered** *bytes* and **logging buffered entries-count** commands are present, then the maximum configured value is taken to display the number of system log messages.

Configuration Example for System Logging Message Count

Use the **logging buffered entries-count** command to specify the number of entries to be present while displaying the system logs.

```
Router# configure
Router(config)# logging buffered entries-count 3000
Router(config)# commit
```

Running Configuration

```
Router#show running-config logging
.
.
.
logging console disable
logging buffered entries-count 3000
!
```

Verification

```
Router(config)#show logging last 3
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level warnings, 2 messages logged
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level informational, 0 messages logged
    Buffer logging: level debugging, 63 messages logged

Log Buffer (3000 entries):
```

Configuring Logging to a Remote Server

Syslog messages can be sent to destinations other than the console, such as logging buffer, syslog servers, snmp servers and terminal lines. You can send syslog messages to an external syslog server by specifying the ip address or hostname of the syslog server using the **logging** command. Also you can configure the syslog facility in which syslog messages are send by using the **logging facility** command.

The following table list the features supported by Cisco IOS XR Software to help managing syslog messages sent to syslog servers.

Table 5: Features for Managing Syslog Messages

Features	Description
UNIX system log facility	Facility is the identifier used by UNIX to describe the application or process that submitted the log message. You can configure the syslog facility in which syslog messages are sent by using the **logging facility** command.
Hostname prefix logging	Cisco IOS XR Software supports hostname prefix logging. When enabled, hostname prefix logging appends a hostname prefix to syslog messages being sent from the router to syslog servers. You can use hostname prefixes to sort the messages being sent to a given syslog server from different networking devices. Use the **logging hostname** command to append a hostname prefix to syslog messages sent to syslog servers

Features	Description
Syslog source address logging	By default, a syslog message sent to a syslog server contains the IP address of the interface it uses to leave the router. Use the **logging source-interface** command to set all syslog messages to contain the same IP address, regardless of which interface the syslog message uses to exit the router.

Configuration Example for Logging to Syslog Server

This example shows the configuration for sending syslog messages to an external syslog server. The ip address 209.165.201.1 is configured as the syslog server.

```
Router# configure
Router(config)# logging 209.165.201.1 vrf default
Router(config)# logging facility kern (optional)
Router(config)# logging hostnameprefix 203.0.113.1 (optional)
Router(config)# logging source-interface HundredGigE 0/0/0/3 (optional)
Router(config)# commit
```

Amongst other options, **all** and **none** are provided under the **logging severity** command form. If you enable **all** or **none**, all or no severity logs are logged to the syslog server, respectively. This configuration persists even when you enable a specific operator type.

Configuration Example for Logging to SNMP Server

This example shows the configuration for sending syslog messages to an SNMP server. The logging trap command is used to limit the logging of messages sent to the snmp servers based on severity.

```
Router# configure
Router(config)# snmp-server traps syslog
Router(config)# logging trap warnings
Router(config)# commit
```

For more information on SNMP server configurations, see the *Configuring Simple Network Management Protocol* chapter in the *System Management Configuration Guide for Cisco NCS 5500 Series Routers*

Related Topics

- Configuring Logging to the Logging Buffer, on page 7
- Configuring Logging to Terminal Lines, on page 12

System Log Facility and Source-address per Remote Server

Table 6: Feature History Table

Feature Name	Release Information	Feature Description
System Log Facility and Source-address per Remote Server	Release 7.10.1	Introduced in this release on:NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) You can now assign a facility number per remote syslog server, which the system inherits to calculate the priority value of the syslog messages sent. You can also configure the source address to choose the interface to send remote syslog packets per remote server. The feature introduces these changes: Modified Command: **CLI** • The keywords **facility** and **source-address** per remote syslog server are introduced in the **logging** command. **YANG Data Models:** • New XPaths for `openconfig-system-logging.yang` (see GitHub, YANG Data Models Navigator)

Configuration Example for Logging to Remote Syslog Server

The configurations for **facility** and **source-address** per remote syslog server takes priority over global configuration.

This example shows how to configure **facility** and **source-address** per remote syslog server:

```
Router#configure
Router(config)#
Router(config)#logging 209.165.201.1 source-address 209.165.201.2
Router(config)#logging 209.165.201.1 facility local2
Router(config)#commit
```

Configuring Logging to Terminal Lines

By default syslog messages will be sent to the console terminal. But, syslog messages can also be send to terminal lines other than the console. You can send syslog messages to the logging buffer using the **logging monitor** command.

Configuration Example

This example shows the configuration for sending syslog messages to terminal lines other than console. In this example, severity level is configured as critical. The terminal monitor command is configured to display syslog messages during a terminal session. The default severity level is debugging.

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# logging monitor critical
RP/0/RP0/CPU0:Router(config)# commit
RP/0/RP0/CPU0:Router# terminal monitor
```

Modifying Logging to Console Terminal

By default syslog messages will be sent to the console terminal. You can modify the logging of syslog messages to the console terminal

Configuration Example

This example shows how to modify the logging of syslog messages to the console terminal.

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# logging console alerts
RP/0/RP0/CPU0:Router(config)# commit
```

Modifying Time Stamp Format

By default, time stamps are enabled for syslog messages. Time stamp is generated in the month day HH:MM:SS format indicating when the message was generated.

Configuration Example

This example shows how to modify the time-stamp for syslog and debugging messages.

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# service timestamps log datetime localtime msec or service
timestamps log uptime
RP/0/RP0/CPU0:Router(config)# service timestamps debug datetime msec show-timezone or service
 timestamps debug uptime
RP/0/RP0/CPU0:Router(config)# commit
```

Suppressing Duplicate Syslog Messages

Suppressing duplicate messages, especially in a large network, can reduce message clutter and simplify the task of interpreting the log. The duplicate message suppression feature substantially reduces the number of duplicate event messages in both the logging history and the syslog file.

Configuration Example

This example shows how to suppress the consecutive logging of duplicate syslog messages.

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# logging suppress duplicates
RP/0/RP0/CPU0:Router(config)# commit
```

Archiving System Logging Messages to a Local Storage Device

Syslog messages can also be saved to an archive on a local storage device, such as the hard disk or a flash disk. Messages can be saved based on severity level, and you can specify attributes such as the size of the archive, how often messages are added (daily or weekly), and how many total weeks of messages the archive will hold. You can create a logging archive and specify how the logging messages will be collected and stored by using the **logging archive** command.

The following table lists the commands used to specify the archive attributes once you are in the logging archive submode.

Table 7: Commands Used to Set Syslog Archive Attributes

Features	Description
archive-length weeks	Specifies the maximum number of weeks that the archive logs are maintained in the archive. Any logs older than this number are automatically removed from the archive.
archive-size size	Specifies the maximum total size of the syslog archives on a storage device. If the size is exceeded then the oldest file in the archive is deleted to make space for new logs.
device {disk0 | disk1 | harddisk}	Specifies the local storage device where syslogs are archived. By default, the logs are created under the directory device**/var/log**. If the device is not configured, then all other logging archive configurations are rejected. We recommend that syslogs be archived to the harddisk because it has more capacity than flash disks.
file-size size	Specifies the maximum file size (in megabytes) that a single log file in the archive can grow to. Once this limit is reached, a new file is automatically created with an increasing serial number.
frequency {daily | weekly}	Specifies if logs are collected on a daily or weekly basis.
severity severity	Specifies the minimum severity of log messages to archive. All syslog messages greater than or equal to this configured level are archived while those lesser than this are filtered out.

Configuration Example

This example shows how to save syslog messages to an archive on a local storage device.

```
Router#conf t
Router(config)#logging archive
Router(config-logging-arch)#device disk1
Router(config-logging-arch)#frequency weekly
Router(config-logging-arch)#severity warnings
Router(config-logging-arch)#archive-length 6
Router(config-logging-arch)#archive-size 50
Router(config-logging-arch)#file-size 10
Router(config-logging-arch)#commit
```

Local Command Accounting

Table 8: Feature History Table

Feature Name	Release Information	Feature Description
Local Command Accounting	Release 7.4.1	This release introduces a new keyword, **local-accounting**, in the **logging file** command, to store the AAA command accounting logs in a user-specified file on the router, in addition to storing them on a remote logging server. When the user enables this feature, the router does not display the command accounting logs in the output of **show logging**, **console logging**, **terminal logging**, or **remote logging**. This release does not support the archiving of local command accounting log files. The modified command is: • logging file *filename* path *pathname* local-accounting

AAA command accounting feature tracks the system activity by generating syslogs for each EXEC command execution. You can also enable local command accounting on the router by configuring the **logging file** command with the **local-accounting** option. When you enable local command accounting, the router stores the AAA command accounting logs in a user-specified log file on the router. These logs aren't visible on the router console, remote-logging server or in the output of the **show logging** command.

For more information about AAA command accounting, refer the *Create Series of Accounting Methods* topic in the *Configuring AAA Services* chapter of the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

Configuring Local Command Accounting

First enable AAA command accounting followed by local command accounting for storing the command accounting logs:

```
Router#conf t
Router(config)#aaa accounting commands default start-stop group tacacs+ local
Router(config)#logging file cmdacctfile path /disk0: maxfilesize 1024 severity info
```

```
local-accounting send-to-remote facility local7
Router(config)#commit
```

Verification steps:

List the files and check for the file you specified in the local command accounting configuration:

```
Router#dir disk0:

Directory of disk0:
24003 drwxr-xr-x. 3 4096 Jun 24 13:14 pam
   20 -rw-r--r--. 1 1414 Jun 24 13:11 envoke_log
16003 drwxr-xr-x. 3 4096 Jun 24 13:12 syslog-hm
24002 drwxr-xr-x. 8 4096 Jun 24 13:13 ztp
   12 drwxr-xr-x. 2 4096 Jun 24 13:11 core
 8001 drwxr-xr-x. 2 4096 Jun 24 13:11 pcie.1
 8003 drwxr-xr-x. 2 4096 Jun 24 13:11 swtam
   65 -rw-r--r--. 1 1536 Jun 24 13:20 cmdacctfile
16001 drwxr-xr-x. 2 4096 Jun 24 13:11 np
16002 drwx---r-x. 2 4096 Jun 24 13:11 clihistory
   22 lrwxrwxrwx. 1   12 Jun 24 13:11 config -> /misc/config
   11 drwx------. 2 4096 Jun 24 13:11 lost+found
 8002 drwxr-xr-x. 2 4096 Jun 24 13:15 pcie
24001 drwxr-xr-x. 2 4096 Jun 24 13:12 crypto
```

To view the contents of the file, use the **more** command:

```
Router#more disk0:cmdacctfile

RP/0/RSP0/CPU0:Jun 24 13:18:11.131 UTC: locald_DLRSC[153]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT
 : CLI CMD: "show running-config" by cisco from TTY /dev/pts/4 console



RP/0/RSP0/CPU0:Jun 24 13:19:07.194 UTC: locald_DLRSC[153]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT
 : CLI CMD: "show logging local location 0/RSP0/CPU0" by cisco from TTY /dev/pts/4 console



RP/0/RSP0/CPU0:Jun 24 13:20:07.071 UTC: locald_DLRSC[153]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT
 : CLI CMD: "dir disk0:" by cisco from TTY /dev/pts/4 console



RP/0/RSP0/CPU0:Jun 24 13:20:35.651 UTC: locald_DLRSC[153]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT
 : CLI CMD: "more disk0:test" by cisco from TTY /dev/pts/4 console
```

Archiving Local Command Accounting Logs

Table 9: Feature History Table

Feature Name	Release Information	Feature Description
Archiving Local Command Accounting Logs	Release 7.5.1	This feature securely stores local command accounting log files that you don't need to access regularly in a specified archive location. Archiving allows you to retain infrequently used log files for operational or regulatory requirements. The associated commands are: • **logging file** *filename* **path** *pathname* **local-accounting** • **logging archive**

For more information on archiving log files, see the topic ***Archiving System Logging Messages to a Local Storage Device*** in this chapter.

Configuring Archiving of Local Command Accounting Logs

Configure local command accounting and **logging archive** in order to enable the archiving of command accounting logs.

The configurations under **logging archive** such as **device**, **frequency**, **severity**, **archive-length**, **archive-size** and **file-size** are common for both system logs and command accounting logs. The router creates separate archive files in the user-specified archive folder for command accounting logs.

Note Except for the **device** configuration, all other configurations under **logging archive** are optional.

If you are configuring **severity** under **logging archive**, then configure it as **informational** because the command accounting logs are informational logs.

Configuration Example for Archiving Local Command Accounting Logs

Configure local command accounting as shown:

```
Router#conf t
Router(config)#aaa accounting commands default start-stop group tacacs+ local
Router(config)#logging file cmdlog1 path disk0: maxfilesize 1024 severity info
local-accounting
Router(config)#commit
```

Configure **logging archive** as shown:

```
Router#conf t
Router(config)#logging archive
Router(config-logging-arch)#device harddisk1
Router(config-logging-arch)#frequency daily
```

```
Router(config-logging-arch)#severity informational
Router(config-logging-arch)#archive-length 6
Router(config-logging-arch)#archive-size 50
Router(config-logging-arch)#file-size 10
Router(config-logging-arch)#commit
```

Verification steps:

In the example above, the router creates a file named **cmdlog1** in **disk0:** for the command accouting logs. The archive for the command accounting log file is created in the path **harddisk:/var/log/***current-date*, which is the archive path for both system logs and command accounting logs.

```
Router#dir disk0:

Directory of disk0:
   65 -rw-r--r--. 1 1536 Sep 20 13:20 cmdlog1

Router#dir harddisk:/var/log/2021/09/20

Directory of harddisk:/var/log/2021/09/20

-rwxr-xr-x. 1 root root 864 Sep 20 23:09 syslog.20.1
-rwxr-xr-x. 1 root root 654 Sep 20 23:09 cmd_accounting_syslog.17.1
```

To view the contents of the archive file, use the **more** command:

```
Router#more cmd_accounting_syslog.17.1

=========Start of Archived syslog file:daily_cmd_log.20210920.17 =========
Router:Sep 20 9:16:38.354 UTC: locald_DLRSC[301]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI
CMD: "show running-config" by lab from TTY /dev/pts/3 console
Router:Sep 20 9:17:54.500 UTC: locald_DLRSC[301]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI
CMD: "show interfaces brief" by lab from TTY /dev/pts/3 console
Router:Sep 20 9:20:50.765 UTC: locald_DLRSC[301]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI
CMD: "admin" by lab from TTY /dev/pts/3 console
Router:Sep 20 9:21:23.301 UTC: locald_DLRSC[301]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI
CMD: "ADMIN 'reload all location 0/RSP0" by lab from TTY con0_RSP0_CPU0 console
=========End of Archived syslog file: daily_cmd_log.20210920.17=========
Router#
```

Platform Automated Monitoring

Platform Automated Monitoring (PAM) is a system monitoring tool integrated into Cisco IOS XR software image to monitor the following issues:

- process crashes
- memory leaks
- CPU hogs
- tracebacks
- disk usage

PAM is enabled by default. When the PAM tool detects any of these system issues, it collects the required data to troubleshoot the issue, and generates a syslog message stating the issue. The auto-collected troubleshooting information is then stored as a separate file in `harddisk:/cisco_support/` or in `/misc/disk1/cisco_support/ directory`.

Table 10: Feature History Table

Feature Name	Release	Description
Platform Automated Monitoring for Blocked Processes	Release 7.5.2	You can enable the Platform Automated Monitoring tool integrated into the Cisco IOS XR software image and receive alerts if any process is blocked. Several system failures can cause a blocked process, such as memory leak, network connection loss, and so on. The tool collects the required data to troubleshoot the issue and generates a system log message with the name of the process that is currently blocked. This feature introduces the following commands: • **enable-pam process-monitoring** • **disable-pam process-monitoring** • **show pam process-monitoring-status**

PAM Events

When PAM detects a process crash, traceback, potential memory leak, CPU hog, a full file system, or blocked process on any node, , it automatically collects logs and saves these logs (along with the core file in applicable cases) as a *.tgz* file in harddisk:/cisco_support/ or in /misc/disk1/cisco_support/ directory. PAM also generates a syslog message with severity level as warning, mentioning the respective issue.

The format of the .tgz file is: *PAM-<platform>-<PAM event>-<node-name>-<PAM process>-<YYYYMMDD>-<checksum>.tgz*.For example, *PAM-ncs5500-crash-xr_0_RP0_CPU0-ipv4_rib-2016Aug16-210405.tgz* is the file collected when PAM detects a process crash.

Because PAM assumes that core files are saved to the default archive folder (harddisk:/ or /misc/disk1/), you must not modify the location of core archive (by configuring exception filepath) or remove the core files generated after PAM detects an event. Else, PAM does not detect the process crash. Also, once reported, the PAM does not report the same issue for the same process in the same node again.

For the list of commands used while collecting logs, refer Files Collected by PAM Tool, on page 21.

The Platform Automated Monitoring for blocked processes detects and alerts if any of the processes are blocked, except for the processes which are blocked by their design. These processes are listed in the table below:

Blocked process	Blocked on
lpts_fm	lpts_pa
isis	lspv_server
Ospf	lspv_server
l2vpn_mgr	lspv_server
mpls_ldp	lspv_server
bgp	lspv_server
te_control	lspv_server
xtc_agent	lspv_server

The sections below describe the main PAM events:

Crash Monitoring

The PAM monitors process crash for all nodes, in real time. This is a sample syslog generated when the PAM detects a process crash:

```
RP/0/RP0/CPU0:Aug 16 21:04:06.442 : logger[69324]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
 crash for ipv4_rib on 0_RP0_CPU0.
All necessary files for debug have been collected and saved at
0/RP0/CPU0 :
harddisk:/cisco_support/PAM-ncs5500-crash-xr_0_RP0_CPU0-ipv4_rib-2016Aug16-210405.tgz
Please copy tgz file out of the router and send to Cisco support. This tgz file will be
removed after 14 days.)
```

Traceback Monitoring

The PAM monitors tracebacks for all nodes, in real time. This is a sample syslog generated when the PAM detects a traceback:

```
RP/0/RP0/CPU0:Aug 16 21:42:42.320 : logger[66139]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
 traceback for ipv4_rib on 0_RP0_CPU0.
All necessary files for debug have been collected and saved at
0/RP0/CPU0 :
harddisk:/cisco_support/PAM-ncs5500-traceback-xr_0_RP0_CPU0-ipv4_rib-2016Aug16-214242.tgz
Please copy tgz file out of the router and send to Cisco support. This tgz file will be
removed after 14 days.)
```

Memory Usage Monitoring

The PAM monitors the process memory usage for all nodes. The PAM detects potential memory leaks by monitoring the memory usage trend and by applying a proprietary algorithm to the collected data. By default, it collects top output on all nodes periodically at an interval of 30 minutes.

This is a sample syslog generated when the PAM detects a potential memory leak:

```
RP/0/RP0/CPU0:Aug 17 05:13:32.684 : logger[67772]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
 significant memory increase
(from 13.00MB at 2016/Aug/16/20:42:41 to 28.00MB at 2016/Aug/17/04:12:55) for
pam_memory_leaker on 0_RP0_CPU0.
All necessary files for debug have been collected and saved at
0/RP0/CPU0 :
harddisk:/cisco_support/PAM-ncs5500-memory_leak-xr_0_RP0_CPU0-pam_memory_leaker-2016Aug17-051332.tgz

(Please copy tgz file out of the router and send to Cisco support. This tgz file will be
removed after 14 days.)
```

CPU Monitoring

The PAM monitors CPU usage on all nodes periodically at an interval of 30 minutes. The PAM reports a CPU hog in either of these scenarios:

- When a process constantly consumes high CPU (that is, more than the threshold of 90 percentage)
- When high CPU usage lasts for more than 60 minutes

This is a sample syslog generated when the PAM detects a CPU hog:

```
RP/0/RP0/CPU0:Aug 16 00:56:00.819 : logger[68245]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
 CPU hog for cpu_hogger on 0_RP0_CPU0.
All necessary files for debug have been collected and saved at 0/RP0/CPU0 :
harddisk:/cisco_support/PAM-ncs5500-cpu_hog-xr_0_RP0_CPU0-cpu_hogger-2016Aug16-005600.tgz
(Please copy tgz file out of the router and send to Cisco support. This tgz file will be
removed after 14 days.)
RP/0/RP0/CPU0:Jun 21 15:33:54.517 : logger[69042]: %OS-SYSLOG-1-LOG_ALERT : PAM detected
ifmgr is hogging CPU on 0_RP0_CPU0!
```

File System Monitoring

The PAM monitors disk usage on all nodes periodically at an interval of 30 minutes. This is a sample syslog generated when the PAM detects that a file system is full:

```
RP/0/RP0/CPU0:Jun 20 13:59:04.986 : logger[66125]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
 /misc/config is full on 0_1_CPU0
(please clean up to avoid any fault caused by this). All necessary files for debug have
been collected and saved at
0/RP0/CPU0 : harddisk:/cisco_support/PAM-ncs5500-disk_usage-xr_0_1_CPU0-2016Jun20-135904.tgz

(Please copy tgz file out of the router and send to Cisco support. This tgz file will be
removed after 14 days.)
```

Disable and Re-enable PAM

The PAM tool consists of the following monitoring processes:

- monitor_cpu.pl
- monitor_crash.pl
- monitor_show_logging.pl
- monitor_process.pl

Note Monitor process.pl in PAM monitors all nodes and generates a system log message with the process name that is blocked if it detects any process is blocked for more than 30 minutes. It prevents multiple alarms for the same blocked process.

Before disabling or re-enabling the PAM, use these options to check if the PAM is installed in the router:

- From Cisco IOS XR Command Line Interface:

```
Router# show pam status
Tue Jun 14 17:58:42.791 UTC
PAM is enabled
```

- From router shell prompt:

```
Router# run ps auxw|egrep perl

root     12559  0.0  0.0  57836 17992 ?        S    Apr24   0:00 /usr/bin/perl
/pkg/opt/cisco/pam//pam_plugin.pl
```

Disable PAM

To disable PAM agent systemwide, execute the following command from XR EXEC mode:

```
Router# disable-pam
```

Re-enable PAM

To re-enable PAM agent systemwide, execute the following command from XR EXEC mode:

```
Router# enable-pam
```

Data Archiving in PAM

At any given point of time, PAM does not occupy more than 200 MB of harddisk: space. If more than 200 MB is needed, then PAM archives old files and rotates the logs automatically.

The PAM collects CPU or memory usage (using **top -b -n1** command) periodically at an interval of 30 minutes. The files are saved under harddisk:/cisco_support/ directory with the filename as <node name>.log (for example, harddisk:/cisco_support/xr-0_RP0_CPU0.log). When the file size exceeds the limit of 15MB, the file is archived (compressed) into .tgz file, and then rotated for a maximum of two counts (that is, it retains only two .tgz files). The maximum rotation count of .tgz files is three. Also, the old file (ASCII data) is archived and rotated if a node is reloaded. For example, xr-0_RP0_CPU0.log is archived if RP0 is reloaded.

You must not manually delete the core file generated by the PAM. The core file is named as *<process name>_pid.by_user.<yyyymmdd>-<hhmmss>.<node>.<checksum>.core.gz*.

Files Collected by PAM Tool

The table below lists the various PAM events and the respective commands and files collected by the PAM for each event.

You can attach the respective.*tgz* file when you raise a service request (SR) with Cisco Technical Support.

Event Name	Commands and Files Collected by PAM
Process crash	• **show install active** • **show platform** • **show version** • core (gz) file • core.txt file
Process traceback	• **show dll** • **show install active** • **show logging** • **show platform** • **show version**
Memory leak	• **show install active** • **show platform** • **show version** • core (gz) file • dumpcore running • continuous memory usage snapshots
Show logging event	• **show install active** • **show logging** • **show platform** • **show version** • core (gz) file • core.txt file

Event Name	Commands and Files Collected by PAM
CPU hog	• **follow process** • **pstack** • **show dll** • **show install active** • **show platform** • **show version** • **top -H** • core (gz) file • CPU usage snapshots
Disk usage	• **show install active** • **show platform** • **show version** • console log • core (gz) file • Disk usage snapshots
Process Blockage	• **show version** • **show install active** • **show platform** • **show logging** • **show running-config** • **show process blocked location all** • core (gz) file

File System Inventory

Table 11: Feature History Table

Feature Name	Release Information	Feature Description
File System Inventory	Release 7.5.1	This feature enables the device to take snapshots of the files inventory at periodic intervals. The metadata of the file includes information about the time that the file was created, last accessed, last modified and so on. A snapshot is captured at each configured interval. These snapshots are collected and stored as inventory data.

This feature enables the device to take snapshots of the files inventory at periodic intervals. The metadata of the file includes information about the time that the file was created, last accessed, last modified and so on. A snapshot is captured at each configured interval. The initial snapshot shows a complete snapshot of all files in the filesystem. Based on the configuration, the files are scanned periodically and new inventory data is collected and stored as full or incremental snapshots. Full snapshots are snapshots which include the entire filesystem for every interval. Whereas incremental snapshots store only the modified files as compared to the previous snapshot based on the interval. You can also configure on-demand snapshots for a specific directory or the entire filesystem.

You can collect the metadata of the filesystem using the data dossier method, operational command method, or using a programmable interface.