Logging

This chapter describes the logging mechanism implemented in the Cisco Identity Services Engine (ISE), including steps to configure logging targets, edit logging categories, and configuring logging settings. The chapter contains the following topics:

Cisco ISE Logging Mechanism

Cisco ISE provides a logging mechanism that is used for auditing, fault management, and troubleshooting. The logging mechanism helps you to identify fault conditions in deployed services and troubleshoot issues efficiently. It also produces logging output from the monitoring and troubleshooting primary node in a consistent fashion.

You can configure a Cisco ISE node to collect the logs in the local systems using a virtual loopback address. To collect logs externally, you configure external syslog servers, which are called targets. Logs are classified into various predefined categories, which are discussed in Cisco ISE Message Codes. You can customize logging output by editing the categories with respect to their targets, severity level, and so on.

You can perform the following logging-related tasks in Cisco ISE:

- To configure local log settings, see Configuring Local Log Purge Settings, page 11-2
- To understand and create remote logging targets, see Cisco ISE System Logs, page 11-2
- To understand and edit logging categories, see Cisco ISE Message Codes, page 11-6
- To view message catalogs, see Cisco ISE Message Catalogs, page 11-7
- To understand and configure debug logs, see Debug Log Configuration Options, page 11-7

Configuring Local Log Purge Settings

Use this process to set local log-storage periods and to delete local logs after a certain period of time.

Step 1 Choose **Administration > System > Logging > Local Log Settings**.

Step 2 In the **Local Log Storage Period** field, enter the maximum number of days to keep the log entries in the configuration source.

Step 3 Click **Delete Logs Now** to delete the existing log files at any time before the expiration of the storage period.

Step 4 Click **Save**.

Cisco ISE System Logs

In Cisco ISE, system logs are collected at locations called logging targets. Targets refer to the IP addresses of the servers that collect and store logs. You can generate and store logs locally, or you can use the FTP facility to transfer them to an external server. Cisco ISE has the following default targets, which are dynamically configured in the loopback addresses of the local system:

- LogCollector—Default syslog target for the Log Collector.
- ProfilerRadiusProbe—Default syslog target for the Profiler Radius Probe.

By default, AAA Diagnostics subcategories and System Diagnostics subcategories logging targets are disabled during a fresh Cisco ISE installation or an upgrade to reduce the disk space. You can configure logging targets manually for these subcategories but local logging for these subcategories are always enabled.

You can use the default logging targets that are configured locally at the end of the Cisco ISE installation or you can create external targets to store the logs. You can create targets only for the subcategories. The parent categories are containers of the subcategories and hence you cannot create targets for them.

Related Topics:

Configuring Remote Syslog Collection Locations, page 11-4

Local Store Syslog Message Format

Log messages are sent to the local store with this syslog message format: *time stamp sequence_num msg_code msg_sev msg_class msg_text attr=value*.

Table 11-1 Local Store and Syslog Message Format

Field	Description
timestamp	Date of the message generation, according to the local clock of the originating the Cisco ISE node, in the format *YYYY- MM-DD hh:mm:ss:xxx +/-zh:zm*. Possible values are: • *YYYY* = Numeric representation of the year. • *MM* = Numeric representation of the month. For single-digit months (1 to 9) a zero precedes the number. • *DD* = Numeric representation of the day of the month. For single-digit days (1 to 9), a zero precedes the number. • *hh* = The hour of the day—00 to 23. • *mm* = The minute of the hour—00 to 59. • *ss* = The second of the minute—00 to 59. • *xxx* = The millisecond of the second—000 to 999. • *+/-zz:zz* = The time zone offset from the Cisco ISE server's time zone, where zh is the number of offset hours and zm is the number of minutes of the offset hour, all of which is preceded by a minus or plus sign to indicate the direction of the offset. For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on a Cisco ISE node that is two hours ahead of the Cisco ISE server's time zone.
sequence_num	Global counter of each message. If one message is sent to the local store and the next to the syslog server target, the counter increments by 2. Possible values are 0000000001 to 999999999.
msg_code	Message code as defined in the logging categories.
msg_sev	Message severity level of a log message (see Logging Category Settings, page A-14).
msg_class	Message class, which identifies groups of messages with the same context.
msg_text	English language descriptive text message.
attr=value	Set of attribute-value pairs that provides details about the logged event. A comma (,) separates each pair. Attribute names are as defined in the Cisco ISE dictionaries. Values of the Response direction AttributesSet are bundled to one attribute called Response and are enclosed in curly brackets {}. In addition, the attribute-value pairs within the Response are separated by semicolons. For example: Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser; cisco-av-pair=sga:security-group-tag=0000-00; }

Configuring Remote Syslog Collection Locations

You can create external locations to store the syslogs.

The UDP SysLog (Log Collector) is the default remote logging target. When you disable this logging target, it no longer functions as a log collector and is removed from the Logging Categories page. When you enable this logging target, it becomes a log collector in the Logging Categories page.

Step 1 Choose **Administration > System > Logging > Remote Logging Targets**.

Step 2 Click **Add**.

Step 3 Configure the field as necessary.

Step 4 Click **Save**.

Step 5 Go to the Remote Logging Targets page and verify the creation of the new target.

After you have created the syslog storage location on logging target page, you should map the storage location to the required logging categories, to receive the logs.

Related Topics

- Remote Logging Target Settings, page A-13

Remote Syslog Message Format

Log messages are sent to the remote syslog server with this syslog message header format, which precedes the local store syslog message format. (see Table 11-1):

pri_num YYYY Mmm DD hh:mm:ss xx:xx:xx:xx/host_name cat_name msg_id total_seg seg_num

The syslog message data or payload is the same as the Local Store Syslog Message Format, which is described in Table 11-1.

Table 11-2 Remote Syslog Message Header Format

Field	Description
pri_num	Priority value of the message; a combination of the facility value and the severity value of the message. Priority value = (facility value* 8) + severity value. The facility code valid options are: • LOCAL0 (Code = 16) • LOCAL1 (Code = 17) • LOCAL2 (Code = 18) • LOCAL3 (Code = 19) • LOCAL4 (Code = 20) • LOCAL5 (Code = 21) • LOCAL6 (Code = 22; default) • LOCAL7 (Code = 23) Severity value—See Setting Severity Levels for Message Codes for severity values.
time	Date of the message generation, according to the local clock of the originating Cisco ISE server, in the format *YYYY Mmm DD hh:mm:ss*. Possible values are: • *YYYY* = Numeric representation of the year. • *Mmm* = Representation of the month—Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • *DD* = Numeric representation of the day of the month. For single-digit days (1 to 9), a space precedes the number. • *hh* = The hour of the day—00 to 23. • *mm* = The minute of the hour—00 to 59. • *ss* = The second of the minute—00 to 59. Some device send messages that specify a time zone in the format -/+hhmm, where - and + identifies the directional offset from the Cisco ISE server's time zone, hh is the number of offset hours, and mm is the number of minutes of the offset hour. For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on a Cisco ISE node that is two hours ahead of the Cisco ISE server's time zone.
xx:xx:xx:xx/host_name	IP address of the originating Cisco ISE node, or the hostname.
cat_name	Logging category name preceded by the `CSCOxxx` string.
msg_id	Unique message ID; 1 to 4294967295. The message ID increases by 1 with each new message. Message IDs restart at 1 each time the application is restarted.

Table 11-2 Remote Syslog Message Header Format (continued)

Field	Description
total_seg	Total number of segments in a log message. Long messages are divided into more than one segment. **Note** The *total_seg* depends on the Maximum Length setting in the remote logging targets page. See Table A-9.
seg_num	Segment sequence number within a message. Use this number to determine what segment of the message you are viewing.

Cisco ISE Message Codes

A logging category is a bundle of message codes that describe a function, a flow, or a use case. In Cisco ISE, each log is associated with a message code that is bundled with the logging categories according to the log message content. Logging categories help describe the content of the messages that they contain.

Logging categories promote logging configuration. Each category has a name, target, and severity level that you can set, as per your application requirement.

Cisco ISE provides predefined logging categories for services, such as Posture, Profiler, Guest, AAA (authentication, authorization, and accounting), and so on, to which you can assign log targets.

See Available Reports, page 26-6 for more information on the relevant troubleshooting reports per category.

Related Topics:

- Setting Severity Levels for Message Codes, page 11-6

Setting Severity Levels for Message Codes

You can set the log severity level and choose logging targets where the logs of selected categories will be stored.

Step 1 Choose **Administration > System > Logging > Logging Categories**.

Step 2 Click the radio button next to the category that you want to edit, and click **Edit**.

Step 3 Modify the required field values.

Step 4 Click **Save**.

Step 5 Go to the Logging Categories page and verify the configuration changes that were made to the specific category.

Related Topics

Logging Category Settings, page A-14

Cisco ISE Message Catalogs

You can use the Message Catalog page to view all possible log messages and the descriptions. Choose **Administration > System > Logging > Message Catalog**.

The Log Message Catalog page appears, from which you can view all possible log messages that can appear in your log files. The data available in this page are for display only.

Debug Log Configuration Options

Debug logs capture bootstrap, application configuration, runtime, deployment, monitoring and reporting, and public key infrastructure (PKI) information.

You can configure the debug log severity level for individual components, and store the debug logs in the local server.

Note A debug log configuration is not saved when a system is restored from a backup or upgraded.

Related Topics

Configuring Debug Log Severity Levels, page 11-7

Configuring Debug Log Severity Levels

You can configure the severity levels for the debug logs.

Step 1 Choose **Administration > System > Logging > Debug Log Configuration**. The Node List page appears, which contains a list of nodes and their personas. You can use the Filter button to search for a specific node, particularly if the node list is large.

Step 2 Select the node, and click **Edit**.

The Debug Log Configuration page contains a list of components that is based on the services that are running in the selected node and the current log level that is set for individual components.

Each node contains a set of components.

Note You can use the Filter button to search for a specific component from the list.

Step 3 Do one of the following to adjust the log severity level:

- Click a component name, choose the desired log severity level from the drop-down list, and click **Save**.
- Choose a component name for which you want to configure the debug log severity level, and click **Edit**. In this page, choose the desired log severity level from the Log Level drop-down list, and click **Save**.

Note Changing the log severity level of *runtime-AAA* component changes the log level of its subcomponent *prrt-JNI* as well. A change in subcomponent log level does not affect its parent component.

Related Topics

- Cisco ISE Support Bundle, page 25-25
- Cisco ISE Debug Logs, page 25-27

Collection Filters

You can configure collection filters to suppress syslog messages being sent to the monitoring and external servers. The suppression can be performed at the Policy Services Node level based on different attribute types. You can disable the suppression as well. You can define multiple filters with a specific attribute type and corresponding value.

Before sending syslog messages to a monitoring node or external server, Cisco ISE compares the values with fields in the syslog messages. If any match is found, then the corresponding message is not sent.

Using Collection Filters

When the Filter is set to **All** or **Passed**, any passed authentication matching the criteria does not show up as Active session and hence license is not consumed. As the passed authentications are not displayed in the Live Session view, you cannot issue a CoA for these sessions. While configuring the collection filters, ensure that you are using them to suppress the syslog events that are not used for monitoring and troubleshooting purposes. This is used to save more disk space, as these events are not recorded.

Related Topics

Configuring Collection Filters, page 11-8

Configuring Collection Filters

You can configure multiple collection filters based on various attribute types. It is recommended to limit the number of filters to 20. You can add, edit, or delete a collection filter.

Step 1 Choose **Administration > System > Logging > Collection Filters**.

Step 2 Click **Add**.

Step 3 Choose the filter type from the **Attribute** list:

- User Name
- MAC Address
- Policy Set Name
- NAS IP Address

- Device IP Address
- Disable Suppression

Step 4 Enter the corresponding **Value** for the filter type you have selected.

Step 5 Choose the result based on which the suppression should be filtered from the **Filter By** drop-down list. The result can be All, Passed, or Failed. You can also choose **Disable Suppression** to disable the suppression.

Step 6 Click **Submit**.

Related Topics

Collection Filters, page 11-8