Manage logging and tracing

NetApp SMI-S Provider

NetApp
June 11, 2024

Table of Contents

Manage logging and tracing

Overview

You can configure how SMI-S Provider manages log and trace files, such as specifying the levels of messages to be logged and the directory to which logs are saved. You also specify the components to be traced, the target to which trace messages are written, the level of tracing, and the trace file location.

Configure log settings

By default, all system messages are logged. In addition, by default, the system message logs are located in the `logs` directory in the directory in which NetApp SMI-S Provider is installed. You can change the location of and the level of system messages that are written to the CIM server log. For example, you can choose to have logs stored in a directory that you specify and have only fatal system messages written to the CIM server log.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

Steps

1. Access NetApp SMI-S Provider.
2. Complete one of the following actions:

Action	Command	Additional information
Change the system message logging level	**cimconfig -s logLevel=*new_log_level* -p**	If you wanted to change the logging level to “INFORMATION”, for example, you would input this command: **cimconfig -s logLevel=INFORMATION -p**
Change the system message log directory	**cimconfig -s logdir=new_log_directory -p** If the *new_log_directory* contains space, you must enclose it in quotation marks (**"***new log directory***"**).	If you wanted to change the log directory to “serverlogs”, for example, you would input this command: **cimconfig -s logdir=serverlogs -p**

3. Restart the CIM server:

   smis cimserver restart

Logging levels

You can specify the types of messages that are logged (for example, you want only fatal system messages to be logged).

You can configure the logging level to one of the following:

- **TRACE**

  Saves trace messages in the cimserver_standard log.

- **INFORMATION**

  Logs all (informational, warning, severe, and fatal) system messages.

- **WARNING**

  Logs warning, severe, and fatal system messages.

- **SEVERE**

  Logs severe and fatal system messages

- **FATAL**

  Logs only fatal system messages.

Manage tracing

You can configure how SMI-S Provider manages trace files, such as specifying the components to be traced, the target to which trace messages are written, the level of tracing, and the trace file location.

Specifying trace settings

Having tracing enabled is important for gathering information for troubleshooting. However, having tracing enabled can impact performance, so carefully consider what must be traced and how long you need tracing enabled.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

Steps

1. Access NetApp SMI-S Provider.
2. Specify various trace settings as applicable:

Action	Command
Specify the components to be traced	**cimconfig -s traceComponents=*components* -p**
Specify the trace facility	**cimconfig -s traceFacility=*facility* -p**
Specify the location of the trace file	**cimconfig -s traceFilePath=*path_name* -p**
Specify the trace level	**cimconfig -s traceLevel=*level* -p**

3. Restart the CIM server:

   smis cimserver restart

Trace setting values

You can specify the components to trace, the trace target, and the level of tracing. Optionally, you can change the name and location of the trace file if you do not want to use the default trace file name and location.

You can configure the following trace settings:

- **traceComponents**

  Specifies the components to be traced. By default, all components are traced.

- **traceFacility**

  Specifies the target to which trace messages are written:

  - File

    This is the default value, which specifies that trace messages are written to the file specified by the traceFilePath configuration option.

  - Log

    Specifies that trace messages are written to the cimserver_standard log file.

- **traceFilePath**

  Specifies the location of the trace file. By default, the trace is file is named `cimserver.trc` and is located in the `traces` directory.

- **traceLevel**

  Specifies the level of tracing. By default, tracing is disabled.

Trace level	Trace messages written
0	Tracing is disabled.
1	Severe and log messages.
2	Basic flow trace messages (low data detail)
3	Inter-function logic flow (medium data detail)
4	High data detail
5	High data detail + Method enter and exit

Specify trace file size

If tracing is enabled, the maximum trace file size is 100 MB by default. You can increase or decrease the maximum trace file size by setting the environment variable `PEGASUS_TRACE_FILE_SIZE`. The value of the trace file size can be 10 MB through 2 GB.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

Steps

1. Access NetApp SMI-S Provider.
2. Create a system or user environment variable named `PEGASUS_TRACE_FILE_SIZE` with the new trace file size in bytes.

   Windows documentation has more information about creating environment variables.

3. Restart the CIM server:

   ```
   smis cimserver restart
   ```

Specify the number of trace files saved

If tracing is enabled, seven trace files are saved by default. If you need more trace files saved, you can increase the maximum number of trace files saved by setting the environment variable `PEGASUS_TRACE_FILE_NUM`. If you increase the maximum number of trace files saved, you must ensure that the system has enough space on its hard drive to accommodate the trace files.

Before you begin

- You must already have login credentials as Administrator.

- You must already have logged in to the host system as Administrator.

About this task

If tracing is enabled, tracing information is written to the `cimserver.trc` file. The trace files are rotated. When `cimserver.trc` reaches the maximum trace file size, its contents are moved to the `cimserver.trc.n` file. By default, `n` is a value from 0 through 5. If you need more trace files saved, you increase the value of *n*.

Steps

1. Access NetApp SMI-S Provider.
2. Create a system or user environment variable named `PEGASUS_TRACE_FILE_NUM` with the new number of trace files saved.

   Windows documentation has more information about creating environment variables.

3. Restart the CIM server:

   `smis cimserver restart`

Enable or disable audit log for SMI-S commands

All incoming SMI-S commands are recorded in audit log files, which enables auditors to track activities of WBEM client operations and provider use. You can enable or disable the logging of these incoming commands by setting a dynamic configuration property.

Before you begin

- You must already have login credentials as Administrator.
- You must already have logged in to the host system as Administrator.

About this task

Audit log data can provide a record of access, activity, and configuration change for a CIM server. The contents of the audit file include what command was issued, by whom the command was issued, and what time the command was issued.

The dynamic configuration property `enableAuditLog` enables or disables audit logging at run time. By default, enableAuditLog is set to true.

The common practice is to leave audit logging enabled.

The audit log file (`cimserver_auditlog`) is stored in the pegasus log directory (`C:\Program Files (x86)\Netapp\smis\pegasus\logs`).

The maximum size of the audit log file is 10 MB. After reaching the maximum limit, the file is renamed `cimserver_auditlog.0`, and a new `cimserver auditlog` file is created to collect the newer audit logging information.

NetApp SMI-S Provider maintains the six most recent audit log files: `cimserver_auditlog.0` through `cimserver_auditlog.5`.

Steps

1. Access NetApp SMI-S Provider.
2. Set the audit logging of SMI-S commands at runtime:

Action	Command
Enable SMI-S audit logging	`cimconfig -s enableAuditLog=true`
Disable SMI-S audit logging	`cimconfig -s enableAuditLog=false`

Copyright information

Trademark information