Monitoring Logs

This chapter includes the following sections:

System Event Log

System Event Log

Cisco UCS Central supports a global system event log (SEL) policy.

The system event log (SEL) records most server-related events, such as over and under voltage, temperature events, fan events, and events from BIOS. The SEL is mainly used for troubleshooting purposes. The SEL file is approximately 40KB in size, and no further events can be recorded when it is full. It must be cleared before additional events can be recorded. You can use the SEL policy to backup the SEL to a remote server, and optionally clear the SEL after a backup operation occurs. Backup operations can be triggered based on specific actions, or they can occur at regular intervals. You can also manually backup or clear the SEL.

System Event Log

The system event log (SEL) resides on the CIMC in NVRAM. It records most server-related events, such as over and under voltage, temperature events, fan events, and events from BIOS. The SEL is mainly used for troubleshooting purposes.

The SEL file is approximately 40KB in size, and no further events can be recorded when it is full. It must be cleared before additional events can be recorded.

You can use the SEL policy to backup the SEL to a remote server, and optionally clear the SEL after a backup operation occurs. Backup operations can be triggered based on specific actions, or they can occur at regular intervals. You can also manually backup or clear the SEL.

The backup file is automatically generated. The filename format is sel-*SystemName-ChassisID-ServerID-ServerSerialNumber-Timestamp*; for example, sel-UCS-A-ch01-serv01-QCI12522939-20091121160736.

Tip For more information about the SEL, including how to view the SEL for each server and configure the SEL policy, see the Cisco UCS Manager configuration guides, which are accessible through the Cisco UCS B-Series Servers Documentation Roadmap.

Configuring the SEL Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope ep-log-policy sel**	Enters organization endpoint log policy mode and scopes the SEL policy.
Step 4	UCSC(policy-mgr) /domain-group/ep-log-policy # **set description** *description*	(Optional) Provides a description for the policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup action** [**log-full**] [**on-change-of-association**] [**on-clear**] [**timer**] [**none**]	Specifies an action or actions that will trigger a backup operation.
Step 6	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup clear-on-backup** {**no** | **yes**}	Specifies whether to clear the system event log after a backup operation occurs.
Step 7	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup destination** *URL*	Specifies the protocol, user, password, remote hostname, and remote path for the backup operation. Depending on the protocol used, specify the URL using one of the following syntax: • **ftp://** *username@hostname* / *path* • **scp://** *username* **@** *hostname* / *path* • **sftp://** *username* **@** *hostname* / *path* • **tftp://** *hostname* **:** *port-num* / *path*

	Command or Action	Purpose
		Note You can also specify the backup destination by using the **set backup hostname** , **set backup password** , **set backup protocol** , **set backup remote-path** , **set backup user** commands, or by using the **set backup destination** command. Use either method to specify the backup destination.
Step 8	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup format** {*ascii* | *binary*}	Specifies the format for the backup file.
Step 9	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup hostname** {*hostname* | *ip-addr*}	Specifies the hostname or IP address of the remote server.
Step 10	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup interval** {**1-hour** | **2-hours** | **4-hours** | **8-hours** | **24-hours** | **never**}	Specifies the time interval for the automatic backup operation. Specifying the **never** keyword means that automatic backups will not be made.
Step 11	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup password** *password*	Specifies the password for the username. This step does not apply if the TFTP protocol is used.
Step 12	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup protocol** {**ftp** | **scp** | **sftp** | **tftp**}	Specifies the protocol to use when communicating with the remote server.
Step 13	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup remote-path** *path*	Specifies the path on the remote server where the backup file is to be saved.
Step 14	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup user** *username*	Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used.
Step 15	UCSC(policy-mgr) /domain-group/ep-log-policy # **commit-buffer**	Commits the transaction.

The following example shows how to configure the SEL policy to back up the system event log (in ascii format) every 24 hours or when the log is full and clear the system event log after a backup operation occurs and commit the transaction

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group #scope ep-log-policy sel
UCSC(policy-mgr) /domain-group/ep-log-policy # set backup destination
scp://user@192.168.1.10/logs
Password:
UCSC(policy-mgr) /domain-group/ep-log-policy* # set backup action log-full
UCSC(policy-mgr) /domain-group/ep-log-policy* #  set backup clear-on-backup yes
UCSC(policy-mgr) /domain-group/ep-log-policy* #  set backup format ascii
UCSC(policy-mgr) /domain-group/ep-log-policy* #  set backup interval 24-hours
```

```
UCSC(policy-mgr) /domain-group/ep-log-policy* #  commit-buffer
UCSC(policy-mgr) /domain-group/ep-log-policy #
```

Configuring Settings for Faults, Events and Logs

Configuring Global Fault Policies

Configuring a Global Fault Policy

Before You Begin

Before configuring a global fault debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create fault policy**	(Optional) If scoping into a domain group previously, creates the fault policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group # **scope fault policy**	(Optional) If scoping into the domain group root previously, scopes the default fault policy's configuration mode from the Domain Group root.
Step 5	UCSC(policy-mgr) /domain-group/policy* # **set ackaction delete-on-clear**	Set the fault policy acknowledgment action to delete on clear (delete-on-clear) or reset to initial severity (reset-to-initial-severity).
Step 6	UCSC(policy-mgr) /domain-group/policy* # **set clearaction delete** | **retain**	Set the fault policy clear action to delete or retain.
Step 7	UCSC(policy-mgr) /domain-group/policy* # **set clearinterval** *clear-number-of-days* | **retain**	Set the fault policy clear interval to the number of days (0-3600) or retain.
Step 8	UCSC(policy-mgr) /domain-group/policy* # **set flapinterval** *flap-number-of-days*	Set the fault policy flap interval to the number of days (0-3600).
Step 9	UCSC(policy-mgr) /domain-group/policy* # **set retentioninterval** *retention-number-of-days* | **forever**	Set the fault policy clear interval to the number of days (0-3600) or forever.

	Command or Action	Purpose
Step 10	UCSC(policy-mgr) /domain-group/policy* # **set soakingseverity condition** | **info** | **warning**	Set the fault policy soaking severity to condition, info, or warning.
Step 11	UCSC(policy-mgr) /domain-group/policy* # **set soakinterval** *soak-number-of-days* | **never**	Set the fault policy soak interval to the number of days (0-3600) or never.
Step 12	UCSC(policy-mgr) /domain-group/policy* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, create a global fault debug policy, enter the status settings, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # create fault policy
UCSC(policy-mgr) /domain-group/policy* # set ackaction delete-on-clear
UCSC(policy-mgr) /domain-group/policy* # set clearaction delete
UCSC(policy-mgr) /domain-group/policy* # set clearinterval 90
UCSC(policy-mgr) /domain-group/policy* # set flapinterval 180
UCSC(policy-mgr) /domain-group/policy* # set retentioninterval 365
UCSC(policy-mgr) /domain-group/policy* # set soakingseverity info
UCSC(policy-mgr) /domain-group/policy* # set soakinterval warning
UCSC(policy-mgr) /domain-group/policy* # commit-buffer
UCSC(policy-mgr) /domain-group/policy #
```

Deleting a Global Fault Debug Policy

A global fault debug policy is deleted from a domain group under the domain group root. Global fault debug policies under the domain groups root cannot be deleted.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **delete fault policy**	Deletes the fault policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the Domain Group domaingroup01, delete the global fault debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group# delete fault policy
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring TFTP Core Export Policies

Core File Exporter

Cisco UCS uses the Core File Exporter to export core files as soon as they occur to a specified location on the network through TFTP. This functionality allows you to export the tar file with the contents of the core file.

Configuring a TFTP Core Export Debug Policy

Before You Begin

Before configuring a TFTP core export debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope tftp-core-export-config**	(Optional) Scopes an existing TFTP Core Export Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group # **create tftp-core-export-config**	(Optional) Creates a TFTP Core Export Debug policy if it does not exist, then scopes into the policy.
Step 5	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **enable core-export-target**	Enables the TFTP core export target.
Step 6	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **set core-export-target path** *name-of-path*	Sets the TFTP core export policy target path.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **set core-export-target port** *port-number*	Sets the TFTP core export policy port number (1-65535).
Step 8	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **set core-export-target server-description** *port-number*	Sets the TFTP core export target policy server description. **Note** Do not use spaces in the server description unless the text is quoted (format examples: "Server description text" or Server_description_text).
Step 9	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **set core-export-target server-name** *server-name*	Sets the TFTP core export target policy server name.
Step 10	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, create the TFTP Core Export Policy, configure the policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create tftp-core-export-config
UCSC(policy-mgr) /domain-group/tftp-core-export-config* # enable core-export-target
UCSC(policy-mgr) /domain-group/tftp-core-export-config* # set core-export-target path /target
UCSC(policy-mgr) /domain-group/tftp-core-export-config* # set core-export-target port 65535
UCSC(policy-mgr) /domain-group/tftp-core-export-config* # set core-export-target
server-description "TFTP core export server 2"
UCSC(policy-mgr) /domain-group/tftp-core-export-config* # set core-export-target server-name
 TFTPcoreserver01
UCSC(policy-mgr) /domain-group/tftp-core-export-config* # commit-buffer
UCSC(policy-mgr) /domain-group/tftp-core-export-config #
```

Deleting a TFTP Core Export Debug Policy

A TFTP core export debug policy is deleted from a domain group under the domain group root. TFTP core export debug policies under the domain groups root cannot be deleted.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /domain-group # **delete tftp-core-export-config**	Deletes the TFTP Core Export Debug policy.
Step 4	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete the TFTP core export debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete tftp-core-export-config
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring Syslog Policies

Configuring a Syslog Debug Policy

Before configuring a syslog debug policy under a domain group, this policy must first be created.

Before You Begin

Syslog Debug Policies under the Domain Group root were created by the system.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the Domain Group root.
Step 3	UCSC(policy-mgr) /domain-group # **create syslog**	Creates a Syslog Debug policy if it does not exist, then scopes into the policy.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, create the Syslog Console Debug Policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create syslog
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/remote-destination #
```

The Syslog Debug Policy is now ready to be configured.

What to Do Next

- Configuring a Syslog Console Debug Policy
- Configuring a Syslog Monitor Debug Policy
- Configuring a Syslog Remote Destination Debug Policy
- Configuring a Syslog Source Debug Policy
- Configuring a Syslog LogFile Debug Policy

Deleting a Syslog Debug Policy

A syslog debug policy is deleted from a domain group under the domain group root. Syslog debug policies under the domain groups root cannot be deleted.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **delete syslog**	Deletes the Syslog Debug policy.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete the Syslog Debug Policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete syslog
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring a Syslog Console Debug Policy

Before configuring a syslog console debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root that were already created by the system are ready to configure.

Before You Begin

Create a Syslog Debug Policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Creates or scopes a Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **create** | **scope console**	Creates or scopes the Syslog Console Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/console* # **enable**	Enables the Syslog Console Debug policy.
Step 6	UCSC(policy-mgr) /domain-group/syslog/console* # **set level 1** | **2** | **0**	Sets the syslog console to one of the following conditions: Alerts (1), Critical (2), or Emergencies (0).
Step 7	UCSC(policy-mgr) /domain-group/syslog/console* # **exit**	Moves back a level for the next create or scope command.
Step 8	UCSC(policy-mgr) /domain-group/syslog/console* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Debug policy, scope the Syslog Console Debug policy, configure the policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog # scope console
UCSC(policy-mgr) /domain-group/syslog/console # enable
UCSC(policy-mgr) /domain-group/syslog/console* # set level 2
UCSC(policy-mgr) /domain-group/syslog/console* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/console #
```

Disabling a Syslog Console Debug Policy

A syslog console debug policy is disabled from a domain group under the Domain Group root. Syslog console debug policies under the Domain Group root cannot be disabled.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Scopes an existing Syslog Console Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **scope console**	Scopes the Syslog Console Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/console* # **disable**	Disables the Syslog Console Debug policy.
Step 6	UCSC(policy-mgr) /domain-group/syslog/console* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope into the Syslog Debug Policy, scope the Syslog Console Debug policy, disable the Syslog Console Debug Policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog* # scope console
UCSC(policy-mgr) /domain-group/syslog/console* # disable
UCSC(policy-mgr) /domain-group/syslog/console* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/console #
```

Configuring a Syslog Monitor Debug Policy

Before configuring a syslog monitor debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root that were already created by the system are ready to configure.

Before You Begin

Create a Syslog Debug Policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root.

	Command or Action	Purpose
		To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Creates or scopes a Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **create** | **scope monitor**	Creates or scopes the Syslog Monitor Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/monitor* # **enable**	Enables the syslog monitor.
Step 6	UCSC(policy-mgr) /domain-group/syslog/monitor* # **set level 1** | **2** | **3** | **4** | **5** | **6** | **7**	Sets the syslog monitor to one of the following conditions: Alerts (1), Cisco UCS domains Critical (2), Cisco UCS domains Major Error (3), Cisco UCS domains Minor Warnings (4), Cisco UCS domains Warning (5), Information (6), Debugging (7).
Step 7	UCSC(policy-mgr) /domain-group/syslog/monitor* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Debug Policy, scope the Syslog Monitor Debug Policy, configure the Syslog Monitor Debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog* # scope monitor
UCSC(policy-mgr) /domain-group/syslog/monitor # enable
UCSC(policy-mgr) /domain-group/syslog/monitor* # set level 3
UCSC(policy-mgr) /domain-group/syslog/monitor* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/monitor #
```

Disabling a Syslog Monitor Debug Policy

A syslog monitor debug policy is disabled from a domain group under the Domain Group root. Syslog monitor debug policies under the Domain Group root cannot be disabled.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Scopes an existing Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **scope monitor**	Scopes the syslog Monitor Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/monitor* # **disable**	Disables the syslog monitor.
Step 6	UCSC(policy-mgr) /domain-group/syslog/monitor* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Debug Policy, scope the Syslog Monitor Debug policy, disable the policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog* # scope monitor
UCSC(policy-mgr) /domain-group/syslog/monitor* # disable
UCSC(policy-mgr) /domain-group/syslog/monitor* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/monitor #
```

Configuring a Syslog Remote Destination Debug Policy

Before configuring a syslog remote destination debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root that were already created by the system are ready to configure.

Before You Begin

Create a Syslog Debug Policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Creates or scopes a Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **create** | **scope remote-destination** | **server-1** | **server-2** | **server-3**	Creates or scopes the Syslog Remote Destination Debug policy to server-1, server-2, or server-3.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /domain-group/syslog/remote-destination* # **enable**	Enables the syslog remote destination.
Step 6	UCSC(policy-mgr) /domain-group/syslog/remote-destination* # **set facility auth** *hostname or level* | **authpriv** *hostname or level* | **cron** *hostname or level* | **daemon** *hostname or level* | **ftp** *hostname or level* | **kernel** *hostname or level* | **local[0-7]** *hostname or level* | **lpr** *hostname or level* | **mail** *hostname or level* | **news** *hostname or level* | **syslog** *hostname or level* | **user** *hostname or level* | **uucp** *hostname or level*	Sets the syslog remote destination facility to the following hostname or level configuration: • Auth • Authpriv • Cron • Daemon • FTP • Kernel • Local0 • Local1 • Local2 • Local3 • Local4 • Local5 • Local6 • Local7 • LPR • Mail • News • Syslog • User • UUCP **Note** • Level is Cisco UCS domains Critical (2), Cisco UCS domains Major Error (3), Cisco UCS domains Minor Warnings (4), Cisco UCS domains Warning (5), Information (6), Debugging (7). • Hostname is 0-255 characters.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /domain-group/syslog/remote-destination* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Debug Policy, scope the Syslog Remote Destination Debug policy, configure the Syslog Remote Destination Debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog* # scope remote-destination server-3
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # enable
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # set facility auth 4
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # set facility auth authhost02
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # set facility authpriv 3
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # set facility auth authprivhost02

  *** Continue configuring all facility settings as required ***
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/remote-destination #
```

Disabling a Syslog Remote Destination Debug Policy

A syslog remote destination debug policy is disabled in a domain group under the domain group root. Syslog remote destination debug policies under the domain groups root cannot be disabled.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Scopes an existing Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **scope remote-destination** | **server-1** | **server-2** | **server-3**	Creates or scopes the Syslog Remote Destination Debug policy to server-1, server-2, or server-3.
Step 5	UCSC(policy-mgr) /domain-group/syslog/remote-destination* # **disable**	Disables the syslog remote destination.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Debug Policy, scope the Syslog Remote Destination Debug policy, disable the Syslog Remote Destination Debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create syslog
UCSC(policy-mgr) /domain-group/syslog* # scope remote-destination server-3
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # disable
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/remote-destination #
```

Configuring a Syslog Source Debug Policy

Before configuring a syslog source debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root that were already created by the system are ready to configure.

Before You Begin

Create a Syslog Debug Policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Creates or scopes a Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **create** | **scope source**	Creates or scopes the Syslog Source Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/source* # **enable**	Enables the syslog source.
Step 6	UCSC(policy-mgr) /domain-group/syslog/remote-destination* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Console Debug Policy, scope the Syslog Source Debug policy, configure the Syslog Source Debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog* # scope source
UCSC(policy-mgr) /domain-group/syslog/source* # enable
UCSC(policy-mgr) /domain-group/syslog/source* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/source #
```

Disabling a Syslog Source Debug Policy

A syslog source debug policy is deleted from a domain group under the domain group root. Syslog source debug policies under the domain groups root cannot be deleted.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group/syslog* # **scope source**	Scopes the Syslog Source Debug policy.
Step 4	UCSC(policy-mgr) /domain-group/syslog/source* # **disable**	Disables the Syslog Source Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/source* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, create the Syslog Console Debug Policy, scope the Syslog Source Debug policy, disable it, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create syslog
UCSC(policy-mgr) /domain-group/syslog* # scope source
UCSC(policy-mgr) /domain-group/syslog/source* # disable
UCSC(policy-mgr) /domain-group/syslog/source* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/source #
```

Configuring a Syslog LogFile Debug Policy

Before configuring a syslog logfile debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root that were already created by the system are ready to configure.

Before You Begin

Create a Syslog Debug Policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Creates or scopes a Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **create** | **scope file**	Creates or scopes the Syslog Logfile Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/file* # **enable**	Enables the syslog logfile.
Step 6	UCSC(policy-mgr) /domain-group/syslog/file* # **set level 1** | **2** | **3** | **4** | **5** | **6** | **7**	Sets the syslog file to one of the following conditions: Alerts (1), Cisco UCS domains Critical (2), Cisco UCS domains Major Error (3), Cisco UCS domains Minor Warnings (4), Cisco UCS domains Warning (5), Information (6), Debugging (7).
Step 7	UCSC(policy-mgr) /domain-group/syslog/file* # **set name** *syslog-file-name*	Sets the syslog file name.
Step 8	UCSC(policy-mgr) /domain-group/syslog/file* # **set size** *syslog-file-size*	Sets the syslog file size (4096-4194304 bytes).
Step 9	UCSC(policy-mgr) /domain-group/syslog/file* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, create the Syslog Debug Policy, scope the Syslog LogFile Debug policy, configure the Syslog Logfile Debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create syslog
UCSC(policy-mgr) /domain-group/syslog* # create file
UCSC(policy-mgr) /domain-group/syslog/file* # enable
UCSC(policy-mgr) /domain-group/syslog/file* # set level 4
UCSC(policy-mgr) /domain-group/syslog/file* # set name syslogfilename01
UCSC(policy-mgr) /domain-group/syslog/file* # set size 4194304
UCSC(policy-mgr) /domain-group/syslog/file* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/file #
```

Disabling a Syslog LogFile Debug Policy

A syslog logfile debug policy is disabled from a domain group under the domain group root. Syslog logfile debug policies under the domain groups root cannot be disabled.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Creates or scopes a Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **scope file**	Scopes the Syslog Logfile Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/file* # **disable**	Disables or enables the syslog logfile.
Step 6	UCSC(policy-mgr) /domain-group/syslog/file* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Debug Policy, scope the Syslog LogFile Debug policy, disable the policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog* # scope file
UCSC(policy-mgr) /domain-group/syslog/file* # disable
UCSC(policy-mgr) /domain-group/syslog/file* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/file #
```