System Management

Managing Power Policies

Cisco UCS Central supports global equipment policies defining the global power allocation policy (based on policy driven chassis group cap or manual blade level cap methods), power policy (based on grid, n+1 or non-redundant methods). Registered Cisco UCS domains choosing to define power management and power supply units globally within that client's policy resolution control will defer power management and power supply units to its registration with Cisco UCS Central.

Creating an Equipment Power 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 sub-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 psu-policy**	Creates the power policy from the domain group.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to create an equipment power policy:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # create psu-policy
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Deleting an Equipment Power Policy

Procedure

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 sub-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 psu-policy**

Deletes the power policy from the domain group.

Step 4 UCSC(policy-mgr) /domain-group* # **commit-buffer**

Commits the transaction to the system.

Example

The following example shows how to delete an equipment power policy:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # delete psu-policy
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring an Equipment Power Policy

Before you begin

Before configuring a power equipment 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 sub-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 psu-policy**	Enters the power policy mode.
Step 4	UCSC(policy-mgr) /domain-group # **set** descr *power-policy-description-text*	Specifies the description for the power policy.
Step 5	UCSC(policy-mgr) /domain-group # **set redundancy grid** | **n-plus-1** | **non-redund**	Specifies the redundancy for the power policy for Grid (grid), N-Plus-1 (n-plus-1), or non-redundancy (non-redund).

Example

The following example scopes the domain group dg1 and configures the equipment power policy for that domain group:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group/psu-policy # set descr "Power policy for sector 24"
UCSC(policy-mgr) /domain-group/psu-policy* # set redundancy grid
UCSC(policy-mgr) /domain-group/psu-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/psu-policy #
```

Viewing an Equipment Power 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 sub-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 # **show psu-policy**	Enters the power policy mode.

Example

The following example shows how to create an equipment power policy:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # scope psu-policy
UCSC(policy-mgr) /domain-group/psu-policy # show
PSU Policy:
    Domain Group Redundancy Description
    ------------ ---------- -----------
    root/dg1     NPlus1
UCSC(policy-mgr) /domain-group #
```

Creating a Global Power Allocation 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 sub-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 cap-policy**	Creates global power allocation policy for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/cap-policy* # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to create a global power allocation policy for a domain group:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # create cap-policy
UCSC(policy-mgr) /domain-group/cap-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/cap-policy #
```

Deleting a Global Power Allocation 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 sub-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 cap-policy**	Deletes global power allocation policy for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/cap-policy* # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to delete a global power allocation policy for a domain group:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # delete cap-policy
UCSC(policy-mgr) /domain-group/cap-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/cap-policy #
```

Configuring a Global Power Allocation Policy for a Chassis Group

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 sub-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 cap-policy**	Enters the global power allocation mode.
Step 4	UCSC(policy-mgr) /domain-group/cap-policy # **set cap-policy policy-driven-chassis-group-cap**	Specifies global power allocation policy for chassis group in the domain group.
Step 5	UCSC(policy-mgr) /domain-group/cap-policy* # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure a global power allocation policy for a chassis group:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) /domain-group # scope domain-group dg1
UCSC(policy-mgr) /domain-group # scope cap-policy
UCSC(policy-mgr) /domain-group/cap-policy # set cap-policy policy-driven-chassis-group-cap

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

Configuring a Global Power Allocation Policy Manually for a Blade Server

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 sub-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 cap-policy**	Enters the global power allocation mode.
Step 4	UCSC(policy-mgr) /domain-group/cap-policy # **set cap-policy manual-blade-level-cap**	Enables manual blade server level power allocation.
Step 5	UCSC(policy-mgr) /domain-group/cap-policy* # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure manual power allocation policy for a blade server:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) /domain-group # scope domain-group dg1
UCSC(policy-mgr) /domain-group # scope cap-policy
UCSC(policy-mgr) /domain-group/cap-policy # set cap-policy manual-blade-level-cap
UCSC(policy-mgr) /domain-group/cap-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/cap-policy #
```

Managing DNS Policies

Cisco UCS Central supports global DNS policies defining the DNS server and domain name. Registered Cisco UCS domains choosing to define DNS management globally within that domain's policy resolution control will defer DNS management to its registration with Cisco UCS Central.

Configuring a DNS Policy

Before you begin

Before configuring a DNS policy in a domain group under the Domain Group root, 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 sub-domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	(Optional) UCSC(policy-mgr) /domain-group # **scope dns-config**	If scoping into the domain group root previously, scopes the default DNS policy's configuration mode from the Domain Group root.
Step 4	(Optional) UCSC(policy-mgr) /domain-group # **create dns-config**	If scoping into a domain group previously, creates the DNS policy for that domain group.
Step 5	UCSC(policy-mgr) /domain-group/dns-config* # **set domain-name** *server-domain-name*	Defines the DNS domain name.
Step 6	UCSC(policy-mgr) /domain-group/dns-config* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Scope into the domain group domaingroup01
- Create the DNS policy for that domain group
- Define the DNS domain name as dnsdomain
- Commit the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create dns-config
UCSC(policy-mgr) /domain-group/domain-group* # set domain-name dnsdomain
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Deleting a DNS 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 a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default DNS policies cannot be deleted under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete dns-config**	Deletes the DNS policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to scope into the domain group domaingroup01, delete the DNS policy for that domain group, and commit the transaction:

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

Configuring a DNS Server for a DNS Policy

Before you begin

Configure a DNS 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 sub-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 dns-config**	Enter an existing DNS policy's configuration mode from the Domain Group root or a domain group scoped into.
Step 4	UCSC(policy-mgr) /domain-group/dns-config # **create dns** server-IP-address	Creates a DNS server instance.
Step 5	UCSC(policy-mgr) /domain-group/dns-config* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Scope into the domain group root
- Create a DNS server instance named 0.0.0.0
- Commit the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # create dns 0.0.0.0
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

The following example shows how to:

- Scope into the domain group domaingroup01
- Create a DNS server instance named 0.0.0.0
- Commit the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # create dns 0.0.0.0
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Deleting a DNS Server from a DNS 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 sub-domain group under the domain

	Command or Action	Purpose
		group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope dns-config**	Enter an existing DNS policy's configuration mode from the Domain Group root or a domain group scoped into.
Step 4	UCSC(policy-mgr) /domain-group/dns-config # **delete dns** *server-IP-address*	Deletes a DNS server instance.
Step 5	UCSC(policy-mgr) /domain-group/dns-config* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Scope into the domain group root
- Delete the DNS server instance named 0.0.0.0
- Commit the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # delete dns 0.0.0.0
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

The following example shows how to:

- Scope into the domain group domaingroup01
- Delete the DNS server instance named 0.0.0.0
- Commit the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # delete dns 0.0.0.0
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Managing Time Zones

Cisco UCS Central supports global date and time policies based on international time zones and defined NTP server. Registered Cisco UCS Manager clients choosing to define date and time globally within that client's policy resolution control will defer the configuration for date and time to its registration with Cisco UCS Central.

Configuring a Date and Time 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 sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	(Optional) UCSC(policy-mgr) /domain-group # **create domain-group** *domain-group*	This step is only necessary to create a new domain group under the Domain Group root (or creates a domain group under the domain group scoped into).
Step 4	(Optional) UCSC(policy-mgr) /domain-group* # **commit-buffer**	This step is only necessary after creating a new domain group under the Domain Group root (or creating a domain group under the domain group scoped into). Commits the new domain group to the system configuration.
Step 5	(Optional) UCSC(policy-mgr) /domain-group # **create timezone-ntp-config**	This step is only necessary the first time a date and time policy is configured for the newly created domain group under the Domain Group root that was created in the previous step, then enter the time zone NTP configuration mode. A date and time policy was created by the system for the Domain Group root, and is ready to be configured.
Step 6	(Optional) UCSC(policy-mgr) /domain-group* # **scope timezone-ntp-config**	This step is only necessary if entering an existing date and time policy's time zone NTP configuration mode from the Domain Group root or a domain group scoped into. Skip this step if creating a date and time policy.
Step 7	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **set timezone**	To set the time zone, press **Enter** after typing the **`set timezone`** command and enter the key value at the prompt. Configures the NTP server time zone. The attribute options are as follows: • **1** —Africa • **2** —Americas • **3** —Antarctica • **4** —Arctic Ocean • **5** —Asia

	Command or Action	Purpose
		• **6** —Atlantic Ocean • **7** —Australia • **8** —Europe • **9** —India Ocean • **10** —Pacific Ocean
Step 8	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Scope the Domain Group root
- Configure the time zone setting to India Ocean ("a continent or ocean") and Maldives ("a country")
- Commit the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 9
Please select a country.
1) British Indian Ocean Territory       7) Maldives
2) Christmas Island                     8) Mauritius
3) Cocos (Keeling) Islands              9) Mayotte
4) Comoros                             10) Reunion
5) French Southern & Antarctic Lands   11) Seychelles
6) Madagascar
#? 7
The following information has been given:
        Maldives
Therefore timezone 'Indian/Maldives' will be set.
Local time is now:      Thu Oct 25 01:58:03 MVT 2012.
Universal Time is now:  Wed Oct 24 20:58:03 UTC 2012.
Is the above information OK?
1) Yes
2) No
#? 1
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to:

- Create a new domain group called domaingroup01 in the Domain Group root
- Commit the transaction
- Create a date and time policy
- Configure the time zone setting to India Ocean ("a continent or ocean") and Maldives ("a country")
- Commit the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # create domain-group domaingroup01
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group # create timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 9
Please select a country.
1) British Indian Ocean Territory       7) Maldives
2) Christmas Island                     8) Mauritius
3) Cocos (Keeling) Islands              9) Mayotte
4) Comoros                             10) Reunion
5) French Southern & Antarctic Lands   11) Seychelles
6) Madagascar
#? 7
The following information has been given:
        Maldives
Therefore timezone 'Indian/Maldives' will be set.
Local time is now:      Thu Oct 25 01:58:03 MVT 2012.
Universal Time is now:  Wed Oct 24 20:58:03 UTC 2012.
Is the above information OK?
1) Yes
2) No
#? 1
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to:

- Scope into domaingroup01 in the Domain Group root
- Create a date and time policy
- Configure the time zone setting to India Ocean ("a continent or ocean") and Maldives ("a country")
- Commit the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr) /domain-group # scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
```

```
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 9
Please select a country.
1) British Indian Ocean Territory       7) Maldives
2) Christmas Island                     8) Mauritius
3) Cocos (Keeling) Islands              9) Mayotte
4) Comoros                             10) Reunion
5) French Southern & Antarctic Lands   11) Seychelles
6) Madagascar
#? 7
The following information has been given:
        Maldives
Therefore timezone 'Indian/Maldives' will be set.
Local time is now:      Thu Oct 25 01:58:03 MVT 2012.
Universal Time is now:  Wed Oct 24 20:58:03 UTC 2012.
Is the above information OK?
1) Yes
2) No
#? 1
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

What to do next

Configure an NTP server for a date and time policy.

Deleting a Date and Time 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 a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default date and time policies cannot be deleted under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete timezone-ntp-config**	Deletes the domain group's time zone policy.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Scope the domain group domaingroup01

- Delete that domain group's date and time policy
- Commit the transaction

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

The following example shows how to:

- Scope the domain group root
- Attempt to delete that domain group's date and time policy
- Commit the transaction
- Recover from an error message (leaving the buffer in an unrecoverable uncommitted state) by initiating a clean exit and reconnecting to the Policy Manager to clear the buffer:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # delete timezone-ntp-config
UCSC(policy-mgr) /domain-group* # commit-buffer
Error: Update failed:
[Timezone and NTP configuration under domain group root cannot be deleted]
UCSC(policy-mgr) /domain-group* # exit
UCSC(policy-mgr)* # exit
UCSC# connect policy-mgr
Cisco UCS Central
UCSC(policy-mgr)#
```

Note In the event you mistakenly scope to the domain group root, and enter the command **delete timezone-ntp-config**, the buffer will encounter an unrecoverable error, remaining in an uncommitted state and preventing subsequent **commit-buffer** commands from saving to the buffer. You must immediately exit and reconnect to the Policy Manager to clear the buffer.

Configuring an NTP Server for a Date and Time 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 sub-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 timezone-ntp-config**	Enters time zone NTP configuration mode.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /domain-group/timezone-ntp-config # **create ntp** *server-name*	Creates an NTP server instance.
Step 5	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Scope into the domain group root
- Create an NTP server instance named domaingroupNTP01
- Commit the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # create ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to:

- Scope into the domain group domaingroup01 under the domain group root
- Create an NTP server instance named domaingroupNTP01
- Commit the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # create ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

What to do next

Configure a date and time policy.

Configuring Properties for an NTP Server

The properties of an NTP server consist of its name. Changing those properties, unlike steps in the GUI involving configuring the NTP server's properties, requires deleting that NTP server and recreating it with a new name.

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 sub-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 timezone-ntp-config**	Enters time zone NTP configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/timezone-ntp-config # **delete ntp** *server-name*	Deletes an NTP server instance that requires renaming.
Step 5	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **create ntp** *server-name*	Creates an NTP server instance to replace the deleted NTP server instance.
Step 6	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Scope into the domain group root
- Delete an NTP server instance named domaingroupNTP01 with a name that is no longer relevant
- Create a new NTP server instance named domaingroupNTP02 to replace the deleted NTP server
- Commit the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # delete ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # create ntp domaingroupNTP02
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

Deleting an NTP Server for a Date and Time 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 sub-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 timezone-ntp-config**	Enters time zone NTP configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/timezone-ntp-config # **delete ntp** *server-name*	Deletes an NTP server instance.
Step 5	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to delete the NTP server instance domaingroupNTP01:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # delete ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to delete the NTP server instance domaingroupNTP01:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # delete ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

Maintenance Policy

A maintenance policy determines how Cisco UCS Central reacts when a change that requires a server reboot is made to a service profile associated with a server or to an updating service profile bound to one or more service profiles.

The maintenance policy specifies how Cisco UCS Central deploys the service profile changes. The deployment can occur in one of the following ways:

- Immediately
- When acknowledged by a user with admin privileges
- Automatically at the time specified in a schedule

If the maintenance policy is configured to deploy the change during a scheduled maintenance window, the policy must include a valid schedule. The schedule deploys the changes in the first available maintenance window.

Note A maintenance policy only prevents an immediate server reboot when a configuration change is made to an associated service profile. However, a maintenance policy does not prevent the following actions from taking place right away:

- Deleting an associated service profile from the system
- Disassociating a server profile from a server
- Directly installing a firmware upgrade without using a service policy
- Resetting the server

Creating a Maintenance Policy

Before you begin

If you plan to configure this maintenance policy for deferred deployment, create a schedule.

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 sub-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 maint-policy** *policy-name*	Creates the specified maintenance policy and enters maintenance policy mode.
Step 4	UCSC(policy-mgr) /domain-group/maint-policy # **set reboot-policy** {**immediate** | **timer-automatic** | **user-ack**}	When a service profile is associated with a server, the server needs to be rebooted to complete the association. Specifying the reboot-policy command determines when the reboot occurs for all service profiles that include this maintenance policy. Possible values include: • **immediate**—The server reboots as soon as the change is made to the service profile. • **timer-automatic** —You select the schedule that specifies when maintenance operations can be applied to the server

	Command or Action	Purpose
		using the **set scheduler** command. Cisco UCS reboots the server and completes the service profile changes at the scheduled time. • **user-ack** —The user must explicitly acknowledge the changes by using the **apply pending-changes** command before changes are applied.
Step 5	(Optional) UCSC(policy-mgr) /domain-group/maint-policy # **enable on-next-boot**	Choose whether to apply the changes on the next reboot, and ignore the selection in the **reboot-policy**.
Step 6	(Optional) UCSC(policy-mgr) /domain-group/maint-policy # **disable on-next-boot**	Disables the **on-next-boot** option.
Step 7	(Optional) UCSC(policy-mgr) /domain-group/maint-policy # **set scheduler** *scheduler-name*	If the reboot-policy property is set to timer-automatic, you must select the schedule that specifies when maintenance operations can be applied to the server. Cisco UCS reboots the server and completes the service profile changes at the scheduled time.
Step 8	(Optional) UCSC(policy-mgr) /domain-group/maint-policy # **set scheduler** *scheduler-name*	If the reboot-policy property is set to timer-automatic, you must select the schedule that specifies when maintenance operations can be applied to the server. Cisco UCS reboots the server and completes the service profile changes at the scheduled time.
Step 9	UCSC(policy-mgr) /domain-group/maint-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Scope into the Domain group root
- Create a maintenance policy called MaintPol1
- Set the system to reboot immediately when a service profile is associated with a server
- Commit the transaction

```
UCSC# connect policy-mgr
UCSC(Policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group# create maint-policy MaintPol1
UCSC(policy-mgr) /domain-group/maint-policy* # set reboot-policy immediate
```

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

Deleting a Maintenance Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete maint-policy** *policy-name*	Deletes the specified maintenance policy.
Step 4	UCSC(policy-mgr) /org #	Commits the transaction to the system configuration.

Example

The following example shows how to delete a maintenance policy called maintenance:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr)/org # delete maint-policy maintenance
UCSC(policy-mgr)/org* # commit-buffer
UCSC(policy-mgr)/org #
```

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 sub-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	(Optional) UCSC(policy-mgr) /domain-group/ep-log-policy # **set description** *description*	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,

	Command or Action	Purpose
		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* **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.

Example

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
- Clear the system event log after a backup operation occurs
- 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 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 sub-domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	(Optional) UCSC(policy-mgr) /domain-group # **create tftp-core-export-config**	Creates a TFTP Core Export Debug policy if it does not exist, then scopes into the policy.
Step 4	(Optional) UCSC(policy-mgr) /domain-group # **scope tftp-core-export-config**	Scopes an existing TFTP Core Export Debug policy's configuration mode.
Step 5	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **enable core-export-target**	Enables the TFTP core export target.

	Command or Action	Purpose
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.
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.

Example

The following example shows how to:

- Scope into the domain group domaingroup01
- Create the TFTP Core Export Policy
- Configure the policy
- 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 #
```

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. The Core File Exporter provides system monitoring and automatic export of core files to be included in TAC cases.

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 sub-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 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.

Example

The following example shows how to delete the TFTP core export debug policy:

```
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 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.

Example

The following example shows how to create the Syslog Console debug policy:

```
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 sub-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 syslog**	Deletes the Syslog Debug policy.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to delete the Syslog debug policy:

```
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 sub-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.

	Command or Action	Purpose
Step 8	UCSC(policy-mgr) /domain-group/syslog/console* # **commit-buffer**	Commits the transaction to the system configuration.

Example

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
- 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

Disable a syslog console debug policy from a sub-domain group. You cannot disable syslog console debug policies under the Domain Group root.

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 sub-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.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /domain-group/syslog/console* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to disable the Syslog Console debug policy:

```
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 sub-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 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).

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

Example

The following example shows how to configure the Syslog Monitor debug policy:

```
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

Disable a syslog monitor debug policy from a domain group under the Domain Group root. You cannot disable a syslog monitor debug policies under the Domain Group root.

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 sub-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 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.

Example

The following example shows how to disable the policy:

```
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 sub-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.
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

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

Example

The following example shows how to configure the Syslog Remote Destination Debug policy:

```
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 hostname 02
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # set facility authpriv 3
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # set facility authpriv hostname
 02
  *** 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 sub-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.

Example

The following example shows how to disable the Syslog Remote Destination debug policy:

```
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* # 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 sub-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.

Example

The following example shows how to configure the Syslog Source Debug policy:

```
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

Delete a syslog source debug policy from a sub-domain group of domain group root. You cannot delete syslog source debug policies under the domain groups root.

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 sub-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.

	Command or Action	Purpose
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.

Example

The following example shows how to disable the Syslog Source Debug policy

```
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.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-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),

	Command or Action	Purpose
		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.

Example

The following example shows how to configure the Syslog Logfile debug policy:

```
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* # 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

Disable a syslog logfile debug policy from a domain group under the domain group root. You cannot diable syslog logfile debug policies under the domain groups root.

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 sub-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.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /domain-group/syslog/file* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to disable the Syslog LogFile debug policy:

```
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 #
```

Enabling Tomcat Logging

Use a terminal emulator to access the CLI.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **scope monitoring**	Enters monitoring mode.
Step 2	UCSC /monitoring # **scope sysdebug**	Enters sysdebug mode.
Step 3	UCSC /monitoring/sysdebug # **scope mgmt-logging**	Enters management logging mode.
Step 4	UCSC /monitoring/sysdebug/mgmt-logging # **set module tomcat_config** [**crit** | **debug0** | **debug1** | **debug2** | **debug3** | **debug4** | **info** | **major** | **minor** | **warn**]	Sets the logging level.
Step 5	UCSC /monitoring/sysdebug/mgmt-logging # **commit-buffer**	Commits the change.

Example

The following example shows how to set tomcat logging to level debug 4.

```
UCSC # scope monitoring
UCSC /monitoring # scope sysdebug
UCSC /monitoring/sysdebug # scope mgmt-logging
UCSC /monitoring/sysdebug/mgmt-logging # set module tomcat_config debug4
UCSC /monitoring/sysdebug/mgmt-logging # commit-buffer
```

Managing High Availability

Cisco UCS Central provides high availability in a cluster setup when you deploy Cisco UCS Central in two virtual nodes. High availability provides stability and redundancy directly to your Cisco UCS Central and indirectly to your Cisco UCS Domains management. The high availability in Cisco UCS Central provides you the following:

- Simplified large scale Cisco UCS deployments with an increased number of servers, chassis, fabric interconnects, and data centers.
- UCS Central VM redundancy in a Hypervisor independent environment.
- A shared storage device to house database and image repositories.
- Built-in failure detection (DME, VM, host, or network failures) and automatic failover to ensure continuous operation.

High Availability Architecture

You will deploy Cisco UCS Central in two VMs on separate hosts to enable high availability. High availability:

- Requires at least one Cisco UCS Manager be registered with Cisco UCS Central for a cluster to support high availability
- Uses the same subnet for individual VMs and VIP addresses
- Allows you to configure a mirrored, multi-path shared storage disk on each VM that is accessible from both hosts
- Uses UCS Manager to store quorum data and determine primary node.
- Exchanges information such as heartbeat and election protocols in the same way as Cisco UCS Manager. This results in a simpler design, more code reusability, and easy to define failover conditions

Cautions and Guidelines for Using High Availability

The following are the guidelines to setup Cisco UCS Central in high availability:

- Make sure both VMs in the cluster should never be on the same server. Otherwise, a single host failure would end up bringing down the cluster.
- Each node in the cluster must have the following:
  - A primary NIC connected to the production network that is used for communicating with Cisco UCS Manager, and for heartbeat communications, with the peer node in the cluster.
  - A host bus adapter connected to the Storage Area Network (SAN), that is used to access the storage target.
- Separate network path for management and storage network.

  Make sure the management network used communications between the two Cisco UCS Central nodes are not on the same network as the network that the nodes use to access the shared disk array. The primary heartbeat mechanism relies on exchanging datagrams across the management network. The secondary

heartbeat mechanism uses quorum data on Cisco UCS Manager. When you use separate network paths for management and shared disk access, that provides redundant paths between the two nodes making it easier to distinguish node failures from link failures.

Note High availability is supported only in IPv4 addressing without the DHCP. You must configure the node IPs and cluster VIPs statically during the installation. These IP addresses are allocated from the production network over which the Cisco UCS Central cluster communicates with Cisco UCS Manager.

- Both VMs must be configured on IP addresses that belongs to the same subnet.
- For NFS, you should configure an NTP server on the NFS server to ensure that the time of both VMs is always synced to Cisco UCS Central.
- Make sure the cluster node infrastructure does not have a single point of failure. You can connect the cluster nodes my multiple, distinct networks. You can also construct the network with redundant switches and routers or similar hardware that removes single points of failure.
- For high availability Cisco UCS Central supports the most commonly used bus types, such as SAS , Fiber Channel (FC), and iSCSI. SCSI compatibility with Persistent Reservations (PRs) is recommended. LUN masking or zoning should be used to isolate the storage volumes accessed by the cluster from other hosts on the network.

Viewing the Cluster State

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show cluster state**	Displays the state of the cluster.

Example

The following example shows how to view the state of a cluster where A is the primary and B the subordinate:

```
UCSC# show cluster state

A: UP, PRIMARY
B: UP, SUBORDINATE

HA NOT READY
No device connected to this VM.
```

Viewing the Extended State of a Cluster

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show cluster extended-state**	Displays the extended state of the cluster.

Example

The following example shows how to view the extended state of a cluster, where A is the primary and B the subordinate:

```
UCSC# show cluster extended-state
Cluster Id: 0x2e95deacbd0f11e2-0x8ff35147e84f3de2

Start time: Thu May 16 06:54:22 2013
Last election time: Thu May 16 16:29:28 2013

A: UP, PRIMARY
B: UP, SUBORDINATE

A: memb state UP, lead state PRIMARY, mgmt services state: UP
B: memb state UP, lead state SUBORDINATE, mgmt services state: UP
   heartbeat state PRIMARY_OK

HA READY
Detailed state of the device selected for HA quorum data:
Device 1007, serial: a66b4c20-8692-11df-bd63-1b72ef3ac801, state: active
Device 1010, serial: 00e3e6d0-8693-11df-9e10-0f4428357744, state: active
Device 1012, serial: 1d8922c8-8693-11df-9133-89fa154e3fa1, state: active
```

Changing the Cluster Lead

Use this command to designate a cluster leader.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect local-mgmt**	Enters local management mode.
Step 2	UCSC(local-mgmt)# **cluster lead** {**a** | **b**}	Change the cluster lead to the specified fabric interconnect. **Note** When the cluster lead changes, the VIP connection will be disconnected. You should log in again to the VIP address, and ensure that it now references the -B node.

Example

The following example shows how to view the primary, change the cluster lead to fabric interconnect B, and verify the result:

```
UCSC-A# show cluster state
Cluster Id: 0x1efd4e4ea47511e5-0x94961118a1af3b76

A: UP, PRIMARY
B: UP, SUBORDINATE

HA NOT READY
No device connected to this VM

UCSC-A# connect local-mgmt
UCSC-A(local-mgmt)# cluster lead b
Cluster Id:0x1efd4e4ea47511e5-0x94961118a1af3b76
UCSC-A(local-mgmt)#
```

After the VIP disconnects, log back in to verify the primary is now fabric interconnect B.

```
UCSC-B# show cluster state
Cluster Id: 0x1efd4e4ea47511e5-0x94961118a1af3b76

B: UP, PRIMARY
A: UP, SUBORDINATE

HA NOT READY
No device connected to this VM

UCSC-B#
```

Force a FI to be Primary

This command forces the secondary FI to be primary. This can be used when the primary FI has failed or remains in Election in Progress state.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect local-mgmt**	Enters local management mode.
Step 2	UCSC(local-mgmt)# **cluster force primary**	Forces the current FI to be the primary.

Example

The following example shows how to use the cluster force primary command:

```
UCSC-A# connect local-mgmt
UCSC-A(local-mgmt)# cluster force primary
Cluster Id:0x1efd4e4ea47511e5-0x94961118a1af3b76

UCSC-A(local-mgmt)#
```

Viewing a Network Interface

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show network-interface**	Displays the network interface information of a cluster.

Example

The following example shows how to view information about the network interface:

```
UCSC# show network-interface
ID   OOB IP Addr     OOB Gateway     OOB Netmask
    ---- --------------- --------------- -----------
    A    10.106.189.54   10.106.189.1    255.255.255.0
    B    10.106.189.55   10.106.189.1    255.255.255.0
```

Viewing Detailed Information about a Network Interface

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show network-interface detail**	Displays the network interface details about a cluster.

Example

The following example shows how to view the detailed network interface information about a cluster:

```
ucsc# show network-interface detail
VM IP interface:
ID: A
    OOB IP Addr: 10.106.189.54
    OOB Gateway:
    OOB Netmask: 255.255.255.0
    Current Task:

ID: B
    OOB IP Addr: 10.106.189.55
    OOB Gateway:
    OOB Netmask: 255.255.255.0
    Current Task:
```

Viewing Network Interface Information of a Server

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show network-interface** *server* [**a** | **b**]	Displays the network information about a server.

Example

The following example shows how to view the network interface information for a server:

```
UCSC# show network-interfaceserver [ a | b]

ID       OOB IP Addr     OOB Gateway     OOB Netmask
    ---- --------------- --------------- -----------
    A    10.106.189.54   10.106.189.1    255.255.255.0
```

Viewing System Information about a Cluster

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show system**	Displays the system information about a cluster.

Example

The following example shows how to view the system information about a cluster:

```
UCSC# show system
Systems:
    Hostname      Installation Type   System IP Address
     ---------------    ----------------------- ----------------------------
    central-vk2      Cluster                  10.106.189.56
central-lun-A#
```

Viewing Detailed System Information about a Cluster

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show system detail**	Displays the system details about the cluster.

Example

The following example shows how to view the system details about a cluster:

```
UCSC# show system detail
System:
    Hostname: central-lun
    Installation Type: Cluster
    System IP Address:
    Current Task:
central-lun-A#
```