# System Management

This chapter includes the following sections:



# Configuring DNS Servers

## 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. |

| | 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 dns-config** | (Optional)<br>If scoping into the domain group root previously, scopes the default DNS policy's configuration mode from the Domain Group root. |
| **Step 4** | UCSC(policy-mgr) /domain-group # **create dns-config** | (Optional)<br>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. |

The following example shows how to scope into the domain group root (which has an existing DNS policy by default), define the DNS domain name as dnsdomain, and 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 # set domain-name dnsdomain
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 the DNS policy for that domain group, define the DNS domain name as dnsdomain, and 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. |

| | Command or Action | Purpose |
|---|---|---|
| | | **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. |

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 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 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. |

The following example shows how to scope into the domain group root, create a DNS server instance named 0.0.0.0, and 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, and 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 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 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. |

The following example shows how to scope into the domain group root, delete a DNS server instance named 0.0.0.0, and 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 a DNS server instance named 0.0.0.0, and 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 Power Allocation

## 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 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. |

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 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 # **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. |

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 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. |

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 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. |

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 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 domain group under the domain group |

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

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 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.

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 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). |

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 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 # **show psu-policy** | Enters the power policy mode. |

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 #
```

# Managing Time Zones

## 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 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 domain-group** *domain-group* | (Optional)<br>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** | UCSC(policy-mgr) /domain-group* # **commit-buffer** | (Optional)<br>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** | UCSC(policy-mgr) /domain-group # **create timezone-ntp-config** | (Optional)<br>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** | UCSC(policy-mgr) /domain-group* # **scope timezone-ntp-config** | (Optional)<br>This step is only necessary if entering an existing date and time policy's time zone NTP configuration mode from the |

| | Command or Action | Purpose |
|---|---|---|
| | | 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:<br>• **1** —Africa<br>• **2** —Americas<br>• **3** —Antarctica<br>• **4** —Arctic Ocean<br>• **5** —Asia<br>• **6** —Atlantic Ocean<br>• **7** —Australia<br>• **8** —Europe<br>• **9** —India Ocean<br>• **10** —Pacific Ocean |
| **Step 8** | UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **commit-buffer** | Commits the transaction to the system configuration. |

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"), and 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 under 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"), and 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 to domaingroup01 under 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"), and 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.<br>**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. |

The following example shows how to scope the domain group domaingroup01, delete that domain group's date and time policy, and 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 and recover from an error message (leaving the buffer in an unrecoverable uncommitted state) by initiating a clean exit and reconnecting to 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 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 # **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. |

The following example shows how to scope into the domain group root, create an NTP server instance named domaingroupNTP01, and 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 to the domain group domaingroup01 under the domain group root, create an NTP server instance named domaingroupNTP01, and 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 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. |

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, and 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 #
```

The following example shows how to scope to the domain group domaingroup01 under 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, and 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 # 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. |
| **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 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. |

The following example shows how to scope the date and time policy in the domain group root, delete the NTP server instance domaingroupNTP01, and 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* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to scope the date and time policy in domaingroup01 under the domain group root, delete the NTP server instance domaingroupNTP01, and 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 # delete ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

# Configuring SNMP

## SNMP Policies

Cisco UCS Central supports global SNMP policies enabling or disabling, defining SNMP traps and SNMP users (with regular and privacy passwords, authentication types of md5 or sha, and encryption types DES and AES-128). Registered Cisco UCS domains choosing to define SNMP policies globally within that client's policy resolution control will defer all SNMP policies to its registration with Cisco UCS Central.

The SNMP Agent functionality provides the ability to remotely monitor the Cisco UCS Central. You can also change the Cisco UCS Central host IP, and then restart the SNMP agent on the new IP. SNMP is run on both the active and standby Cisco UCS Central servers and the configuration is persisted on both. Cisco UCS Central offers read-only access to only the operating system managed information base (MIB).Through the Cisco UCS Central CLI you can configure the community strings for SNMP v1, v2c, and create and delete the SNMPv3 users.

## SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within Cisco UCS Central, the managed device, that maintains the data for Cisco UCS Central and reports the data, as needed, to the SNMP manager. Cisco UCS Central includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP in Cisco UCS Central.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent. Cisco UCS Central supports only the OS MIBs.

Cisco UCS Central supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. The following RFCs define the SNMP:

- RFC 3410 (http://tools.ietf.org/html/rfc3410)
- RFC 3411 (http://tools.ietf.org/html/rfc3411)
- RFC 3412 (http://tools.ietf.org/html/rfc3412)
- RFC 3413 (http://tools.ietf.org/html/rfc3413)
- RFC 3414 (http://tools.ietf.org/html/rfc3414)
- RFC 3415 (http://tools.ietf.org/html/rfc3415)
- RFC 3416 (http://tools.ietf.org/html/rfc3416)
- RFC 3417 (http://tools.ietf.org/html/rfc3417)
- RFC 3418 (http://tools.ietf.org/html/rfc3418)
- RFC 3584 (http://tools.ietf.org/html/rfc3584)

## SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

Cisco UCS Central generates SNMP notifications as traps. Traps are less reliable because the SNMP manager does not send any acknowledgment when it receives a trap, and Cisco UCS Central cannot determine if the trap was received.

## SNMP Security Features

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages. The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur non-maliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality and encryption—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

## SNMP Security Levels and Privileges

SNMPv1, SNMPv2c, and SNMPv3 each represent a different security model. The security model combines with the selected security level to determine the security mechanism applied when the SNMP message is processed.

The security level determines the privileges required to view the message associated with an SNMP trap. The privilege level determines whether the message needs to be protected from disclosure or authenticated. The supported security level depends upon which security model is implemented. SNMP security levels support one or more of the following privileges:

- noAuthNoPriv—No authentication or encryption
- authNoPriv—Authentication but no encryption
- authPriv—Authentication and encryption

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

## SNMP Security Models and Levels

The following table describes the combinations of SNMP security models and levels supported in Cisco UCS Central.

***Table 1: SNMP Security Models and Levels***

| Model | Level | Authentication | Encryption | What Happens |
|---|---|---|---|---|
| v1 | noAuthNoPriv | Community string | No | Uses a community string match for authentication. |

| Model | Level | Authentication | Encryption | What Happens |
|---|---|---|---|---|
| v2c | noAuthNoPriv | Community string | No | Uses a community string match for authentication. |
| v3 | noAuthNoPriv | Username | No | Uses a username match for authentication. |
| v3 | authNoPriv | HMAC-MD5 or HMAC-SHA | No | Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA). |
| v3 | authPriv | HMAC-MD5 or HMAC-SHA | DES | Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard. |

# SNMP Support in Cisco UCS Central

### Support for MIBs

Cisco UCS Central supports read-only access to OS MIBs. No set operations are available for the MIBs. The following MIBs are supported by Cisco UCS Central:

- SNMP MIB-2 System
- HOST-RESOURCES-MIB
  - hrSystem
  - hrStorage

    - hrDevice
    - hrSWRun
    - hrSWRunPerf
- UCD-SNMP-MIB
    - Memory
    - dskTable
    - systemStats
    - fileTable
- SNMP MIB-2 Interfaces
    - ifTable
- IP-MIB
- SNMP-FRAMEWORK-MIB
    - snmpEngine
- IF-MIB
- DISMAN-EVENT-MIB
- SNMP MIB-2 snmp

**Note** Cisco UCS Central does not provide support for IPV6 andCisco UCS Central MIBs.

### Authentication Protocols for SNMPv3 Users

Cisco UCS Central supports the following authentication protocols for SNMPv3 users:

- HMAC-MD5-96 (MD5)
- HMAC-SHA-96 (SHA)

### AES Privacy Protocol for SNMPv3 Users

Cisco UCS Central uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826. If AES is disabled but privacy password is set, then DES is used for encryption.

If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, Cisco UCS Central uses the privacy password to generate a 128-bit AES key. The AES privacy password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters.

# Configuring an SNMP Policy

## Before You Begin

Before configuring a SNMP 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 snmp** | (Optional)<br>If scoping into a domain group previously, creates the SNMP policy for that domain group. |
| **Step 4** | UCSC(policy-mgr) /domain-group # **scope snmp** | (Optional)<br>If scoping into the domain group root previously, scopes the default SNMP policy's configuration mode from the Domain Group root. |
| **Step 5** | UCSC(policy-mgr) /domain-group/snmp* # **enable** \| **disable snmp** | Enable or disable SNMP services for this policy. |
| **Step 6** | UCSC(policy-mgr) /domain-group/snmp* # **set community** *snmp-community-name-text* | Enter a name for the SNMP community. |
| **Step 7** | UCSC(policy-mgr) /domain-group/snmp* # **set syscontact** *syscontact-name-text* | Enter a name for the SNMP system contact. |
| **Step 8** | UCSC(policy-mgr) /domain-group/snmp* # **set syslocation** *syslocation-name-text* | Enter a name for the SNMP system location. |
| **Step 9** | UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to scope into the Domain Group root, scope the SNMP policy, enable SNMP services, set the SNMP community name to SNMPCommunity01, set the SNMP system contact name to SNMPSysAdmin01, set the SNMP system location to SNMPWestCoast01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # enable snmp
UCSC(policy-mgr) /domain-group/snmp* # set community SNMPCommunity01
UCSC(policy-mgr) /domain-group/snmp* # set syscontact SNMPSysAdmin01
UCSC(policy-mgr) /domain-group/snmp* # set syslocation SNMPWestCoast01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

The following example shows how to scope into the Domain Group domaingroup01, create the SNMP policy, enable SNMP services, set the SNMP community name to SNMPCommunity01, set the SNMP system contact name to SNMPSysAdmin01, set the SNMP system location to SNMPWestCoast01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create snmp
UCSC(policy-mgr) /domain-group/snmp* # enable snmp
UCSC(policy-mgr) /domain-group/snmp* # set community SNMPCommunity01
UCSC(policy-mgr) /domain-group/snmp* # set syscontact SNMPSysAdmin01
UCSC(policy-mgr) /domain-group/snmp* # set syslocation SNMPWestCoast01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

The following example shows how to scope into the domain group domaingroup01, scope the SNMP policy, disable SNMP services, and commit the transaction:

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

## Configuring an SNMP Trap

### 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 snmp** | Scopes the default SNMP policy's configuration mode. |
| **Step 4** | UCSC(policy-mgr) /domain-group/snmp # **create snmp-trap** *snmp-trap-ip* | (Optional)<br>If scoping into a domain group previously, creates the snmp-trap IP address for that domain group (in format 0.0.0.0), and enters SNMP trap configuration mode. |
| **Step 5** | UCSC(policy-mgr) /domain-group/snmp # **scope snmp-trap** *snmp-trap-ip* | (Optional)<br>If scoping into the domain group root previously, scopes the snmp-trap IP address for that domain group (in format 0.0.0.0), and enters SNMP trap configuration mode. |
| **Step 6** | UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set community** *snmp-trap-community-host-config-string* | Enter the SNMP trap community string to configure the SNMP trap host. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set notificationtype traps** | Enter the notification type for the SNMP trap as SNMP Trap Notifications (traps). |
| **Step 8** | UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set port** *port-number* | Enter the SNMP trap port number (1-65535). |
| **Step 9** | UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set v3privilege auth** \| **noauth** \| **priv** | Enter a V3 Privilege security level for the SNMP trap of authNoPriv Security Level (auth), noAuthNoPriv Security Level (noauth), or authPriv Security Level (priv). |
| **Step 10** | UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set version v1** \| **v2c** \| **v3** | Enter a version for the SNMP trap of SNMP v1, v2c, or v3. |
| **Step 11** | UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to scope into the Domain Group root, scope the SNMP policy, create the SNMP trap with IP address 0.0.0.0, set the SNMP community host string to snmptrap01, set the SNMP notification type to traps, set the SNMP port to 1, set the v3privilege to priv, set the version to v1, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # create snmp-trap 0.0.0.0
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set community snmptrap01
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set notificationtype traps
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set port 1
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set v3privilege priv
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set version v1
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-trap #
```

The following example shows how to scope into the domain group domaingroup01, scope the SNMP policy, scope the SNMP trap IP address 0.0.0.0, set the SNMP community host string to snmptrap02, set the SNMP notification type to traps, set the SNMP port to 65535, set the v3privilege to auth, set the version to v2c, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # scope snmp-trap 0.0.0.0
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set community snmptrap02
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set notificationtype traps
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set port 65535
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set v3privilege auth
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set version v2c
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-trap #
```

# Configuring an SNMP User

## 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 snmp** | Scopes the SNMP policy's configuration mode. |
| **Step 4** | UCSC(policy-mgr) /domain-group/snmp # **create snmp-user** *snmp-user* | Enter a name for the SNMP user. |
| **Step 5** | UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set aes-128 yes** \| **no** | Use AES-128 for the SNMP user (yes or no). |
| **Step 6** | UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set auth md5** \| **sha** | Use MD5 or Sha authorization mode for the SNMP user. |
| **Step 7** | UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set password** *password* | Enter and confirm a password for the SNMP user. |
| **Step 8** | UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set priv-password** *private-password* | Enter and confirm a private password for the SNMP user. |
| **Step 9** | UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to scope into the Domain Group root, scope the SNMP policy, scope into the SNMP user named snmpuser01, set aes-128 mode to enabled, set authorization to sha mode, set password to userpassword01, set private password to userpassword02, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # scope snmp-user snmpuser01
UCSC(policy-mgr) /domain-group/snmp/snmp-user # set aes-128 yes
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set auth sha
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set password userpassword01
Enter a password: userpassword01
Confirm the password: userpassword01
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set priv-password userpassword02
Enter a password: userpassword02
Confirm the password: userpassword02
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # commit-buffer
```

```
UCSC(policy-mgr) /domain-group/snmp/snmp-user #
```

The following example shows how to scope into the domain group domaingroup01, scope the SNMP policy, create the SNMP user named snmpuser01, set aes-128 mode to enabled, set authorization to md5 mode, set password to userpassword01, set private password to userpassword02, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # create snmp-user snmpuser01
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set aes-128 yes
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set auth md5
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set password userpassword01
Enter a password: userpassword01
Confirm the password: userpassword01
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set priv-password userpassword02
Enter a password: userpassword02
Confirm the password: userpassword02
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-user #
```

The following example shows how to scope into the Domain Group root, scope the SNMP policy, scope into the SNMP user named snmpuser01, set aes-128 mode to disabled, set authorization to md5 mode, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # scope snmp-user snmpuser01
UCSC(policy-mgr) /domain-group/snmp/snmp-user # set aes-128 no
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set auth md5
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-user #
```

## Deleting an SNMP Policy

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

Deleting an SNMP policy will remove all SNMP trap and SNMP User settings within that 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.<br>**Note** Do not enter the domain group root itself. System default Management Interfaces Monitoring policies cannot be deleted under the domain group root. |
| **Step 3** | UCSC(policy-mgr) /domain-group # **delete snmp** | Deletes the SNMP 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 SNMP policy, and commit the transaction:

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

## Deleting an SNMP Trap

### 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 snmp** | Scopes the default SNMP policy's configuration mode. |
| **Step 4** | UCSC(policy-mgr) /domain-group/snmp # **delete snmp-trap** *snmp-trap-ip* | Deletes the snmp-trap IP address for that domain group. |
| **Step 5** | UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to scope into the Domain Group root, scope the SNMP policy, delete the SNMP trap IP address 0.0.0.0, and commit the transaction:

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

The following example shows how to scope into the domain group domaingroup01, scope the SNMP policy, delete the SNMP trap IP address 0.0.0.0, and commit the transaction:

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

## Deleting an SNMP User

### 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 snmp** | Scopes the SNMP policy's configuration mode. |
| **Step 4** | UCSC(policy-mgr) /domain-group/snmp # **delete snmp-user** *snmp-user* | Delete the SNMP user. |
| **Step 5** | UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows how to scope into the Domain Group root, scope the SNMP policy, delete the SNMP user named snmpuser01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp snmpuser01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

The following example shows how to scope into the Domain Group domaingroup01, scope the SNMP policy, delete the SNMP user named snmpuser02, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp snmpuser02
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

# Managing High Availability

## About High Availability in Cisco UCS Central

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 UCS Central cluster communicates with UCSMs.

- Both VMs must be configured on IP addresses that belongs to the same subnet.
- 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. |

The following example shows how to view the state of a cluster:

```
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** *cluster ID* | Displays the extended state of the cluster. |

The following example shows how to view the extended state of a cluster:

```
UCSC# show cluster extended-state 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
```

# Viewing a Network Interface

### Procedure

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

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. |

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. |

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. |

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. |

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#
```