Log and Trace Settings

View List of Host Addresses for Configured Devices

Use the **Log and Trace Settings** page to see the list of Host Addresses for all configured devices and to configure log and trace settings for those devices.

The host address for the Controller displays two processes - OAMPserver and the name for the Unified Intelligence Center Reporting server processes running on the controller.

From the **Actions** column, click the ellipsis icon (...) to edit the Log, Syslog, and Subsystem server connection settings for that server process.

Logging and Tracing

Logging and Tracing are two mechanisms for application monitoring and management and are differentiated as follows:

- Logs contain predefined, higher-level messages that can indicate everything from general system behavior to severe error conditions.

- Traces are free-form, developer-oriented, detailed information that is not printed to the logs by default, but only when increased logging is enabled to debug problems.

You configure log levels to be *Basic* or *Detailed*. *Basic* is the default. When you change the log levels to *Detailed*, you have the opportunity to select specific trace level definitions.

There are two ways to review log and tracing information:

- The *Command Line Interface*. Using the show trace command.

- The *Real Time Monitoring Tool* (RTMT).

Related Topics

Real Time Monitoring Tool

Command Line Interface

Edit Syslog Server Connection Settings

From the **Log and Trace Settings** list page > **Actions** column, click the ellipsis icon (...) and click **Edit** to edit the Log, Syslog, and Subsystem settings.

⚠

Caution Modify the settings on this page only under the direction of, and with the assistance of, your support provider.

Log Settings

Use the following required fields to define the maximum size of the log directory and of each log file.

Field	Description
Maximum Log Directory Size	Enter a numeric value between 50 and 50,000. The default is 1,500. When the directory size exceeds 50,000, the oldest log files are deleted.
Maximum Log File Size	Enter a numeric value between 1 and 50. The default is 50. When a log size exceeds 50, a new log file is created.

Syslog Settings

Use the following fields to identify the server where the log files are stored.

✎

Note You must restart the Unified Intelligence Center server for the change to take effect.

Field	Description
Primary Host	The host address of the primary syslog server that stores the log files. **Note** The port is fixed at 514.
Backup Host	The host address of the backup syslog server that stores the log files. **Note** The port is fixed at 514.

Subsystem Settings

Click the **Subsystem** tab to set the log levels for each subsystem. For more information, see *Log Levels and Trace Level Definitions: Basic and Detailed*.

Actions on this page

- **Save** - Save the changes you have made.

- **Cancel** - Undo all changes you have made since the last save.

Related Topics

Log Levels and Trace Level Definitions: Basic and Detailed

There are two log levels for all subsystems:

Basic

This is the default log level. With this setting, messages and warnings are displayed (INFO, ERROR, and WARN).

When the log level is Basic, the trace definitions are not editable.

Detailed

If you check the detailed log level, the trace check boxes for Subsystem Specific Trace Definitions and Infrastructure Trace Definitions become editable. You can check the boxes to turn on specific trace code paths to output to the log file.

There are two ways to review log and trace information:

- The *Command Line Interface* (show trace).

- The *Real Time Monitoring Tool* (RTMT).

Related Topics

> Real Time Monitoring Tool

Infrastructure Trace Definitions

Infrastructure Trace definitions are the same for Unified Intelligence Center and for Operation Administration Maintenance and Provisioning (OAMP) Infrastructure and OAMP_BO. There are no Infrastructure Trace Definitions for OAMP WSM_BO.

Trace	Description
TRACE_HANDLED_EXCEPTION	Description of the exception and how it was handled
TRACE_JMX	JMX and management interface related traces
TRACE_PARAM	For any parameters (not just method arguments)
TRACE_CALL	For traces related to a call / call processing
TRACE_GENERAL_CFG	General traces for configuration API
TRACE_OOOQUEUE	Set this bit to enable OoOQueue tracing
TRACE_METHOD	When entering and exiting a method
TRACE_LOW_LEVEL	Bits and Bytes

OAMP

Operation Administration Maintenance and Provisioning (OAMP) Subsystem Specific Trace Definitions

Trace	Definition
TRACE_BULK	To control logging for looping/bulk operations
TRACE_GENERAL_UI	For tracing the general OAMP UI
TRACE_EXCEPTION	For tracing Exceptions
TRACE_PARAM	For tracing Parameters
TRACE_DBACCESS	Trace DB Access for db fetch and modify such as Save, Update, Delete
TRACE_METHOD	For tracing of Entry/Exit of Methods

Infrastructure

Infrastructure Subsystem Specific Trace Definitions

Trace	Description
TRACE_HANDLED_EXCEPTION	Description of the exception and how it was handled
TRACE_JMX	JMX and management interface related traces
TRACE_PARAM	For any parameters (not just method arguments)
TRACE_CALL	For traces related to a call / call processing
TRACE_GENERAL_CFG	General traces for configuration API
TRACE_OOOQUEUE	Set this bit to enable OoOQueue tracing
TRACE_METHOD	When entering and exiting a method
TRACE_LOW_LEVEL	Bits and Bytes

OAMP-BO

OAMP-BO Subsystem Specific Trace Definitions

Trace	Description
TRACE_BULK	To control logging for looping/bulk operations
TRACE_EXCEPTION	For tracing Exceptions
TRACE_GENERAL_BO	General Traces for OAMP back-end
TRACE_PARAM	For tracing Parameters
TRACE_DBACCESS	Trace DB Access for db fetch and modify such as Save, Update, Delete

Trace	Description
TRACE_METHOD	For tracing of Entry/Exit of Methods

WSM-BO

WSM-BO Subsystem Specific Trace Definitions

Trace	Description
TRACE_EXCEPTION	For tracing Exceptions
TRACE_GENERAL_BO	General Traces for OAMP back-end
TRACE_PARAM	For tracing Parameters
TRACE_DBACCESS	Trace DB Access for db fetch and modify such as Save, Update, Delete
TRACE_METHOD	For tracing of Entry/Exit of Methods

CUIC

CUIC Subsystem Specific Trace Definitions

CUIC Subsystem, Cache, Thread, Schedule, Util, Statistics, JMX, I18N, L10N, Message, Help

Trace	Definition
CUIC_SUBSYS_SETUP	Trace for CuicSubsystem setup
CUIC_SUBSYS_OBJECT	Trace for CuicSubsystem object dump

Infrastructure

Infrastructure Subsystem Specific Trace Definitions

Trace	Description
TRACE_HANDLED_EXCEPTION	Description of the exception and how it was handled
TRACE_JMX	JMX and management interface related traces
TRACE_PARAM	For any parameters (not just method arguments)
TRACE_CALL	For traces related to a call / call processing
TRACE_GENERAL_CFG	General traces for configuration API
TRACE_OOOQUEUE	Set this bit to enable OoOQueue tracing
TRACE_METHOD	When entering and exiting a method

Trace	Description
TRACE_LOW_LEVEL	Bits and Bytes

CUIC Model Objects

CUIC Model Objects Specific Trace Definitions for Reports, Report Definitions, Templates, Dashboards, folders, Value Lists, and Collections.

Trace	Description
MODEL_DASHBOARD	Trace dashboard objects
MODEL_DATA_SOURCE	Trace data source objects
MODEL_REPORT_DEFINITION	Trace report definition objects
MODEL_COLLECTION	Trace collection objects
MODEL_REPORT	Trace report objects
MODEL_VALUE_LIST	Trace value list objects

CUIC Data Processing

CUIC Data Processing Subsystem Specific Trace Definitions for Data Source, Data Processing, and Hibernate.

Trace	Description
DCP	Trace for DCP other than worker threads
DCP_WORKER	Trace for DCP worker threads

CUIC Security

CUIC Data Processing Subsystem Specific Trace Definitions for Encryption, Permission, User, Group, and ICM User Synchronization.

Trace	Description
PERMISSION_OPERATION	Trace for security operation details
PERMISSION_OBJECT	Trace for security object details

IP Address and Hostname of Cisco Unified Intelligence Center Nodes

Warning Perform the IP address change only during a maintenance window.

This section provides the steps to change the IP address or hostname on a Cisco Unified Intelligence Center server. You may want to change this IP address for a variety of reasons, which include moving the server from one segment to another or resolving a duplicate IP address problem.

IP Address Change Checklist

Perform the following tasks to ensure that your system is prepared for a successful IP address change.

If you have a DNS configured anywhere on the Unified Intelligence Center servers, ensure the following before changing the IP address:

- There is a forward and reverse lookup zone configured.

- The DNS is reachable and working.

Note If you do not receive the results that you expect when you perform these tasks, do not continue with this procedure until after you resolve any problems that you find.

Prepare for IP Address Change

You must perform the following tasks before changing the IP address.

Procedure

Step 1 List all servers in the cluster and note whether the nodes are defined by using IP addresses or host names.
  a) From the Administration console on the first node, navigate to **Device Configuration**. System displays a list of all servers in the cluster.
  b) Capture this list of servers for later reference.

Step 2 Ensure that you have saved an inventory of both the host name and IP address of each node in your cluster.

Step 3 Ensure that all servers in the cluster are up and available by checking for any active ServerDown alerts. You can check by using either the Real Time Monitoring Tool (RTMT) or the Command Line Interface (CLI) on the first node.

- To check by using RTMT, access Alert Central and check for ServerDown alerts.

- To check by using the CLI on the first node, enter the following command and inspect the application event log:

```
file search activelog syslog/CiscoSyslog ServerDown
```

Step 4   Check the DB replication status on all the Unified Intelligence Center nodes in the cluster to ensure that all servers are replicating database changes successfully. You can check by using either RTMT or a CLI command.

- To check by using RTMT, access the Database Summary and inspect the replication status.

- To check by using the CLI, enter the command that is shown in the following example:

```
admin: show perf query class "Number of Replicates Created and State of Replication"
==>query class :
- Perf class (Number of Replicates Created and State of Replication)
has instances and values:
ReplicateCount -> Number of Replicates Created = ###
ReplicateCount -> Replicate_State = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

- 0-Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service is not running and has not been running since the subscriber was installed.

- 1-Replicates have been created, but their count is incorrect.

- 2-Replication is good.

- 3-Replication is bad in the cluster.

- 4-Replication setup did not succeed.

Step 5   To check network connectivity and DNS server configuration, enter the CLI command that is shown in the following example:

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1log
Starting diagnostic test(s)
===================================
test - validate network : Passed
Diagnostics completed
admin:
```

Step 6   Run a manual DRS backup and ensure that all nodes and active services are backed up successfully. For more information, see *Disaster Recovery System*.

Related Topics
Disaster Recovery System

Change Cluster IP Addresses for Subscriber Servers Defined by IP Addresses

Use this procedure to change the IP address of a subscriber server if your cluster servers are defined by an IP address. To successfully change the IP address, you must complete all steps in this procedure.

Note   To define subscriber servers on the Cisco Unified Intelligence Center publisher server or to determine how a subscriber server is defined, navigate to **Device Configuration**.

Procedure

Step 1　From the OAMP, choose **Device Configuration**. The system opens **Find and List Servers** window.

Step 2　Select the subscriber server from the **Find and List Servers** window.

Step 3　Change the IP address of the subscriber server to reflect the new IP address.

Step 4　Ensure that the IP address change is replicated to the subscriber server database by entering the CLI command `run sql select * from mmca_device` on all nodes in the cluster. The following example shows the command output:

```
name               nodeid
================== ======
EnterpriseWideData  1
10.3.90.21          4
10.3.90.5           2
```

Step 5　If you are moving the subscriber server to a different subnet that requires a new default gateway address, change the default gateway by using the set network gateway CLI command, as shown in the following example:

```
admin: set network gateway 10.3.90.2
*** W A R N I N G ***
This will cause the system to temporarily lose network connectivity
Do you want to continue ?
Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

Step 6　Change the IP address of the subscriber server by performing the following tasks:

> **Note**　When you are logging in to the subscriber server to perform this step, ensure that you use the original IP address of the subscriber server and not the IP address that you changed in the publisher node.

a) Enter the complete CLI command `set network ip eth0 ip_address netmask gateway` where `ip_address` specifies the new server IP address, `netmask` specifies the new server network mask and `gateway` specifies the new server network gateway.

The following output displays:

```
***   W A R N I N G   ***
If there are Member(Subscriber) IP addresses (not hostnames)
configured in Cisco Unified Intelligence Center Administration
under Device Management -> Device Configuration
then you must change the IP address there BEFORE
changing it here .
This will cause the system to restart
========================================================
 Note: To recognize the new IP address all nodes within
       the cluster will have to be manually rebooted.
========================================================
```

b) Enter `Yes` and press **Enter**.

> **Note**　You can also change the IP address of the default gateway and the subscriber server by using the Cisco Unified Communications Operating System. From Cisco Unified Communications Operating System Administration, choose **Settings** > **IP** > **Ethernet**.

Step 7   Ensure that your updated subscriber server restarts after this step. If it does not, manually reboot the server for the changes to take effect.

> **Note**   These files get updated only during system startup; the system needs to restart core network services, a Cisco DB and Cisco Tomcat, after the files are updated. Restarting the servers ensures the proper update and service-restart sequence for the IP address changes to take effect.

Step 8   When changing the IP address of more than one subscriber server, do the following:

a) Change the IP address for one server.
b) Reboot the cluster.
c) Check the replication status.

   If the changed IP address reflects properly, follow the same procedure on the next subscriber server. Otherwise do not change the IP address of the other servers.

   Caution: Avoid doing the changes in parallel in several servers at the same time, as it can lead to .rhosts, sqlhosts files being out of sync in the cluster.

Change Cluster IP Address for Publisher Server Defined by IP Address

Use this procedure to change the IP address of a publisher server if your cluster servers are defined by an IP address.

> **Note**   You cannot use this procedure to change a subscriber's host publisher server from one publisher server to another publisher server.

Procedure

Step 1   From the Cisco Unified Operating System Administration window of each subscriber server in the cluster, perform the following tasks:

a) Navigate to **Settings** > **IP** > **Publisher.**
b) Change the IP address of the publisher server.

Step 2   If you are moving the server to a different subnet that requires a new default gateway address, change the default gateway by using the set network gateway CLI command, as shown in the following example:

```
admin: set network gateway 10.3.90.2
*** W A R N I N G ***
This will cause the system to temporarily lose network connectivity
Do you want to continue ?
Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

Step 3   To change the IP address of the publisher server, perform one of the following tasks:

To change the IP address from Cisco Unified Operating System Administration:

a. Choose **Settings** > **IP** > **Ethernet.**

      b. Enter the new IP addresses.

      c. Click **Save**. The server reboots automatically.

To change the IP address by using a CLI command

      a. Enter the complete CLI command `set network ip eth0 ip_address netmask gateway` where `ip_address` specifies the new server IP address, `netmask` specifies the new server network mask and `gateway` specifies the new server gateway.

      b. Follow the prompt and press **Enter.**

Step 4 Ensure that the IP address change is replicated to the subscriber server database by entering the CLI command run sql select * from mmca_device on all nodes in the cluster. The following example shows the command output:

```
name               nodeid
================== ======
EnterpriseWideData   1
10.3.90.21           4
10.3.90.5            2
```

Step 5 After the publisher server reboots automatically, reboot all subscriber servers to update the local name resolution files, such as hosts, rhosts, sqlhosts, and services.

| **Note** | These files get updated only during system startup, and the system needs to restart core network services, such as Cisco DB and Cisco Tomcat, after the files are updated. Restarting the servers ensures the proper update and service-restart sequence for the IP address changes to take effect. |

Step 6 Run a manual DRS backup and ensure that all nodes and active services get backed up successfully. For more information, see *Disaster Recovery System*.

Related Topics

    Disaster Recovery System

Change Cluster IP Addresses for Subscriber Servers Defined by Host Name

Use this procedure to change the IP address of a subscriber server if your cluster servers are defined by a host name.

⚠️

| **Caution** | Be aware that a DRS backup that you take from a server with a particular host name cannot be restored on a server (either a publisher or subscriber node) with a different host name, even after you reinstall that node. |

Procedure

Step 1 Change the DNS record of the subscriber server to point to the new IP address. Ensure that you correctly update both the forward (A) and reverse (PTR) records. You must refresh your DNS cache to ensure that the records get correctly updated.

Note	DNS servers comprise part of the network infrastructure. Unified Intelligence Center servers do not and cannot run DNS services.

Step 2 Verify that the DNS change propagates to other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all the cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11
admin:show tech network hosts
------------------ show platform network --------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 3 If you are moving the server to a different subnet that requires a new default gateway address, change the default gateway by using the `set network gateway` CLI command, as shown in the following example:

```
admin:set network gateway 10.3.90.2
            *** W A R N I N G ***
This will cause the system to temporarily lose network connectivity
Do you want to continue ?
Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

Step 4 Change the IP address of the subscriber server by performing the following tasks:

a) Enter the complete CLI command `set network ip eth0 ip_address netmask gateway` where `ip_address` specifies the new server IP address, `netmask` specifies the new server network mask and `gateway` specifies the new server network gateway.

The following output displays:

```
*** W A R N I N G ***
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
then you must change the IP address there BEFORE
changing it here or call processing will fail.
This will cause the system to restart
=======================================================
Note: To recognize the new IP address all nodes within
the cluster will have to be manually rebooted.
=======================================================
Do you want to continue?
Enter "yes" to continue and restart or any other key to abort
```

    b) Enter `yes` and press **Enter**.

Note	You can also change the IP address of the default gateway and the server by using the Cisco Unified Communications Operating System. From Cisco Unified Communications Operating System Administration, choose **Settings** > **IP** > **Ethernet**.

Step 5   Reboot all other servers in the cluster, including the publisher server, to update the local name resolution files, such as hosts, rhosts, sqlhosts, and services.

Note	These files only get updated during system startup; you need to restart core network services, such as Cisco DB and Cisco Tomcat, after the files are updated. Restarting the servers ensures that the proper update and service-restart sequence for the IP address changes take effect.

Step 6   Do the following if you want to change the IP address of more than one subscriber server:

    a) Change the IP address for one server.

    b) Reboot the cluster.

    c) Check the replication status. If the changed IP address reflects properly, follow the same procedure on the next subscriber server. Otherwise do not change the IP address of the other servers.

Warning	Avoid making the changes in parallel in several servers at the same time, because doing so can lead to .rhosts, sqlhosts files being out of sync in the cluster.

Step 7   Verify that the DNS change propagates to other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all the cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11
admin:show tech network hosts
------------------- show platform network --------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 8   Run a manual DRS backup and ensure that all nodes and active services get backed up successfully. For more information, see *Disaster Recovery System*.

Related Topics

    Disaster Recovery System

Change Cluster IP Address for Publisher Server Defined by Host Name

Use this procedure to change the IP address of a publisher server if your servers are defined by a host name.

⚠️

Caution   Be aware that a DRS backup that you take from a server with a particular host name cannot be restored on a server (either a publisher or subscriber node) with a different host name, even after you reinstall that node.

Procedure

Step 1   Change the DNS record of the publisher server to point to the new IP address. Ensure that you correctly update both the forward (A) and reverse (PTR) records.

> **Note**   DNS servers comprise part of the network infrastructure. Unified Intelligence Center servers do not and cannot run DNS services.

Step 2   Verify that the DNS change propagates to other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all the cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11
admin:show tech network hosts
------------------- show platform network -------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 3   From the Cisco Unified Communications Operating System Administration window (`https://subscriber_ip_address/cmplatform`) of each subscriber server in the cluster, perform the following tasks:

a) Navigate to **Settings** > **IP** > **Publisher**.
b) Change the IP address of the publisher server.

Step 4   If you are moving the server to a different subnet that requires a new default gateway address, change the default gateway by using the `set network gateway` CLI command, as shown in the following example:

```
admin:set network gateway 10.3.90.2
*** W A R N I N G ***
This will cause the system to temporarily lose network connectivity
Do you want to continue ?
Enter "yes" to continue or any other key to stop
yes
```

```
executing...
admin:
```

Step 5 Change the IP address of the publisher server by using the CLI by performing the following tasks:

a) Enter the complete CLI command `set network ip eth0 ip_address netmask gateway` where `ip_address` specifies the new server IP address, `netmask` specifies the new server network mask and `gateway` specifies the new server network gateway.

The following output displays:

```
*** W A R N I N G ***
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
then you must change the IP address there BEFORE
changing it here or call processing will fail.
This will cause the system to restart
========================================================
Note: To recognize the new IP address all nodes within
the cluster will have to be manually rebooted.
========================================================
Do you want to continue?
Enter "yes" to continue and restart or any other key to stop
```

b) Enter `Yes` and press **Enter**.

> **Note** You can also change the IP address of the default gateway and the server by using the Cisco Unified Communications Operating System. From Cisco Unified Communications Operating System Administration, choose **Settings** > **IP** > **Ethernet**.

Step 6 After the publisher server reboots automatically as a result of the `set network ip` command, reboot all subscriber servers to update the local name resolution files, such as hosts, rhosts, sqlhosts, and services.

> **Note** These files only get updated during system startup, and you need to restart core network services, such as Cisco DB and Cisco Tomcat, after the files are updated. Restarting the servers ensures that the proper update and service-restart sequence for the IP address changes take effect.

Step 7 Ensure that local resolution of the subscriber node also resolves to the new IP address by running the `utils network host` and `show tech network hosts` CLI commands:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11
admin:show tech network hosts
------------------- show platform network --------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 8   Run a manual DRS backup and ensure that all nodes and active services get backed up successfully. For more information, see *Disaster Recovery System*.

Related Topics

[Disaster Recovery System](#)

Change Hostname for Unified Intelligence Center Publisher (Controller) Node

This section describes how to change the hostname for the Unified Intelligence Center Publisher (Controller) Node that is defined by an IP address.

Procedure

Step 1   Change the DNS record of the subscriber server to point to the new IP address. If the IP address is being changed at the same time, ensure that the DNS servers also reflect the IP address. Ensure that forward (A) and reverse (PTR) records update correctly.

Note: DNS servers comprise part of the network infrastructure. Unified Intelligence Center servers don't and can't run DNS servers.

Step 2   If the server for which you're changing the hostname is a publisher server, log on to each subscriber server in the cluster and change the hostname mapping of the cluster Publisher server. You can perform this task from Cisco Unified Operating System Administration or by using a CLI command.

To change the mapping from Unified Intelligence Center Operating System Administration, log in to each subscriber server in the cluster and perform the following tasks:

Step 3   Change the hostname of the server from Cisco Unified Operating System Administration:

a)   Navigate to **Settings** > **IP** > **Ethernet**.
b)   Change the hostname to the new hostname.
c)   Click **Save**. The server automatically reboots with the new changes.

Note   Changing the hostname triggers an automatically self-signed certificate regeneration. If your cluster is using CA-signed certificates, you must have them re-signed. For regenerating SAML certificate, refer to the **Hostname or IP Address Change** section in the [Cisco Unified Contact Center Enterprise Features Guide](#).

Step 4   If the IP address changes along with the hostname and the server moves to a new subnet, change the server Default Gateway to the new address by using the `set network gateway ip address` CLI command.

If the default gateway changes, before the next step, ensure that the server moves to the new subnet and has access to the default gateway. During Unified Intelligence Center server startup, the Verify Network script checks server access to the default gateway. If the server can't communicate with the default gateway at startup time, the Verify Network script fails and start up may be delayed. If you're using Manual DHCP configuration and the DHCP server isn't reachable or doesn't give out an IP address to the server, the system won't boot; instead, the system continues to wait at the Verify Network startup phase.

Step 5   Reboot all other servers in the cluster twice, including the publisher.

Step 6   Verify that the name-IP association change that was made in Step 4 propagates to the other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all cluster nodes.

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11
admin:show tech network hosts
------------------- show platform network ------------------- /etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

You can also use the `utils diagnose module validate_network` command on all cluster nodes. This diagnostics module checks that you configured DNS client services correctly, that the server can connect to the DNS server, and that Forward (A) and Reverse (PTR) records are present and match the server IP address and hostname.

Note   Don't proceed until the change propagates to all nodes.

Step 7   From the publisher server, run the CLI `utils dbreplication stop all` to stop the automatic setup of database replication and to stop ongoing setup of replication.

Step 8   For all the nodes in the cluster, run `utils dbreplication dropadmindb`.

Step 9   From the publisher server, run `utils dbreplication reset all` to set up replication across the whole cluster again.

Change Hostname for Unified Intelligence Center Subscriber (Member) Node

This section describes how to change the hostname for Unified Intelligence Center Subscriber (Member) Nodes that are defined by an IP address in Unified Intelligence Center.

Procedure

Step 1   Change the DNS record of the subscriber server to point to the new IP address. If the IP address is being changed at the same time, ensure that the DNS servers also reflect the IP address. Ensure that forward (A) and reverse (PTR) records update correctly.

Note   DNS servers comprise part of the network infrastructure. Unified Intelligence Center servers do not and cannot run DNS services.

Step 2   From the Unified Intelligence Center Administration console page, perform the following tasks:

a) Navigate to **Device Configuration**.

b) Change the Host Address of the subscriber node to the new hostname.

c) Click the **Save** button.

Step 3 To change the hostname of Unified Intelligence Center subscriber (Member) node, log in to Cisco Unified Operating System Administration page on each subscriber node in the cluster and perform the following tasks:

a) Navigate to **Settings** > **IP** > **Ethernet**.

b) Change the hostname to the new hostname.

c) Click **Save**. The server automatically reboots with the new changes.

Step 4 To change the hostname using a CLI command:

a) Enter the CLI command `set network hostname hostname`.

b) Enter **Yes** and press **Enter**. This command automatically reboots this server with the new hostname.

Step 5 Reboot all other servers in the cluster twice, including the publisher.

Step 6 Verify that the name-IP association change that was made in Step 3 propagates to the other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all cluster nodes.

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11admin
.
.
.
cups114.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Note   You can also use the `utils diagnose module validate_network` command on all cluster nodes. This diagnostics module checks that you configured DNS client services correctly, that the server can connect to the DNS server, and that Forward (A) and Reverse (PTR) records are present and match the server IP address and hostname.

Note   Do not proceed until the change propagates to all nodes.

Step 7 From the publisher server, run the CLI `utils dbreplication stop all` to stop the automatic setup of database replication and to stop ongoing setup of replication.

Step 8 From the publisher server, run `utils dbreplication reset all` to set up replication across the whole cluster again.

Verify IP Address Change

After you finish changing the IP addresses of your cluster, complete the following tasks.

Procedure

Step 1 Ensure that all servers in the cluster are up and available by checking for any active ServerDown alerts. You can check by using either the Real Time Monitoring Tool (RTMT) or the Command Line Interface (CLI) on the first node.

a) To check by using RTMT, access Alert Central and check for ServerDown alerts.

b) To check by using the CLI on the first node, enter the following command and inspect the application event log: `file search activelog syslog/CiscoSyslog ServerDown`

Step 2 Check the DB replication status on all Unified Intelligence Center nodes in the cluster to ensure that all servers are replicating database changes successfully. You can check by using either RTMT or a CLI command.

To check by using RTMT, access the Database Summary and inspect the replication status.

To check by using the CLI, enter the command that the following example shows:

```
admin: show perf query class "Number of Replicates Created and State of Replication"
==>query class :
- Perf class (Number of Replicates Created and State of Replication)
has instances and values:
ReplicateCount -> Number of Replicates Created = 344
ReplicateCount -> Replicate_State = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

- 0 - Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service has not been running since the subscriber was installed.

- 1- Replicates have been created, but their count is incorrect.

- 2 - Replication is good.

- 3 - Replication is bad in the cluster.

- 4 - Replication setup did not succeed.

Step 3   Run a manual DRS backup and ensure that all nodes and active services backed-up successfully.

Step 4   Update RTMT custom alerts and saved profiles:

- RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure these custom alerts.

- RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and re-add these counters and then save the profile to update it to the new IP address.

Configure IPv6

Cisco Unified Intelligence Center supports IPv6 using dual stack (IPv4 and IPv6). You can enable IPv6 after installation using the either Cisco Unified Communications Operating System Administration or CLI.

With IPv6 enabled, the Unified Intelligence Center Administration Console and REST APIs can connect to the Unified Intelligence Center server using IPv4 or IPv6.

Note   After installation, if you are not using IPv6 or IPv6 address is not assigned, disable the IPv6 service.

Set up IPv6 using CLI

To set up IPv6 using the CLI, perform the following procedure on the primary and secondary servers of Unified Intelligence Center.

Procedure

Step 1   Access the CLI on the Unified Intelligence Center server.

Step 2 To enable or disable IPv6, enter: **set network ipv6 service {enable | disable}**.

Step 3 Set the IPv6 address and prefix length : **set network ipv6 static_address** *addr mask*. Example: set network ipv6 static_address 2001:db8:2::a 64

Step 4 Set the default gateway : **set network ipv6 gateway** *addr*

Step 5 Restart the system for the changes to take effect : **utils system restart**

Step 6 To display the IPv6 settings, enter : **show network ipv6 settings**

The IPv6 configured is global.

Set up IPv6 using Cisco Unified Communications Operating System Administration

To set up IPv6 using Cisco Unified Operating System Administration, perform the following procedure on both the primary and secondary Unified Intelligence Center servers.

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration on the Unified Intelligence Center server (https://*host or IP address*/cmplatform, where *host or IP address* is the hostname or IP address of the Unified Intelligence Center server).

Step 2 Navigate to **Settings** > **IP** > **Ethernet IPv6**.

Step 3 To enable IPv6, check the **Enable IPv6** check box (or uncheck the box to disable IPv6).

Step 4 Enter values for **IPv6 Address**, **Subnet Mask**, and **Default Gateway**.

Step 5 To restart after you save the changes, check the **Update with Reboot** check box. Click **Save**