Change IP Address and Hostname

IP Address and Hostname Overview

You can change the network-level IP address and hostname name of nodes in your deployment for a variety of reasons, including moving the node from one network domain to another or resolving a duplicate IP address problem. The IP address is the network-level Internet Protocol (IP) associated with the node, and the Hostname is the network-level hostname of the node.

This document provides detailed procedures for the following tasks for Cisco Emergency Responder nodes:

- Change the IP address of a node
- Change the hostname of a node

Task lists are provided for each of these procedures that summarize the steps to perform.

Use the *Cisco Emergency Responder 10.5(1) Command Line Interface Guide* to assist you when changing an IP Address or Hostname. This guide replaces the chapter previously found in the Cisco Emergency Responder Administration Guide.

The Emergency Responder Command Line Interface Guide can be found on the Cisco Emergency Responder Command Reference page.

Note You must complete all pre-change tasks and system health checks before you make these changes, and you must complete the post-change tasks after you make any of these changes.

Pre-Change Tasks and System Health Checks

The following sections discuss pre-change tasks and system health checks. You must perform these tasks before you change a Hostname or IP address.

Pre-Change Task List for Cisco Emergency Responder Nodes

The following table lists the tasks to perform before you proceed to change the IP address and hostname for Cisco Unified Communications Manager nodes. You must perform these procedures during a scheduled maintenance window. Perform all system health checks before you perform the pre-change setup tasks.

For details about any of the tasks that are listed, see topics related to performing system health checks on nodes and pre-change setup.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Item	Task
System health checks	
1.	If you have DNS configured anywhere on the Cisco Emergency Responder servers, ensure that forward and reverse records (for example, a record and PTR record) are configured and that the DNS is reachable and working.
2.	Ensure that all servers in the cluster are up and available, and check for any active ServerDown alerts.
3.	Check the database replication status of all Cisco Emergency Responder nodes in the cluster to ensure that all servers are replicating database changes successfully.
4.	Check network connectivity and DNS server configuration.
Pre-change setup tasks	
5.	Use Cisco Emergency Responder Administration to compile a list of all nodes in the cluster. Retain this information for use later.
6.	Run a manual Disaster Recovery System backup and ensure that all nodes and active services are backed up successfully. For more information, see the *Disaster Recovery System Administration Guide* for your release.

Check System Health

Perform the applicable system health checks on the nodes in your deployment as part of the pre-change setup and as part of the post-change tasks that you must perform after you have changed any network identifiers.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Some of the checks in this procedure are required only for post-change verification. See the post-change task list for a complete list of the system health checks to perform.

Note If you are performing system health checks as part of the pre-change setup, you can skip the following steps which are only required when you are performing the post-change tasks:

- Verification that the new hostname or IP address appears on the Cisco Emergency Responder server list.
- Verification that changes to the IP address, hostname, or both are fully implemented in the network.
- Verification that changes to the hostname is fully implemented in the network.

Procedure

Step 1 If you have DNS configured anywhere on the Cisco Emergency Responder servers, ensure that a forward and reverse lookup zone has been configured and that the DNS is reachable and working.

Step 2 Check for any active ServerDown alerts to ensure that all servers in the cluster are up and available. Use the command line interface (CLI) on the first node.

a) Enter the following CLI command on the first node and inspect the application event log: **file search activelog syslog/CiscoSyslog ServerDown**.

Step 3 Check the database replication status on all nodes in the cluster to ensure that all servers are replicating database changes successfully.

Use CLI to get status of DB replication.

To check using the CLI, enter **utils dbreplication status**.

For example output, see topics related to example database replication output. For detailed procedures and troubleshooting, see topics related to verifying database replication and troubleshooting database replication.

Step 4 Enter the CLI command **utils diagnose** as shown in the following example to check network connectivity and DNS server configuration.

```
admin:utils diagnose module validate_network

Log file: platform/log/diag1.log

Starting diagnostic test(s)
===========================
test - validate_network    : Passed

Diagnostics Completed
```

The final output will be in Log file: platform/log/diag1.log.

Use **file view activelog platform/log/diag1.log** command to see the output.

Step 5 If you are performing the pre-change system health checks, you are done; otherwise, continue to perform the post-change verification steps.

Step 6 Verify that the new hostname or IP address appears on the Unified Communications Manager server list. In Cisco Unified CM Administration, select **System > Server Settings**.

Note Perform this step only as part of the post-change tasks.

Step 7 Verify that changes to the IP address, hostname, or both are fully implemented in the network. Enter the CLI command **show network cluster** on each node in the cluster. Perform this step only as part of the post-change tasks.

Note The output should contain the new IP address or hostname of the node.

Example

```
admin:show network cluster
10.77.29.191 cer-191-p123.cisco.com cer-191-p123 Publisher callmanager DBPub authenticated
10.77.29.192 cer186-sub.cisco.com cer186-sub Subscriber ciscoer DBSub authenticated using
TCP since Fri Oct 10 18:42:40 2014


Successful
```

Step 8 Verify that changes to the hostname are fully implemented in the network. Enter the CLI command **utils network host <new_hostname>** on each node in the cluster.

Perform this step only as part of the post-change tasks.

Note The output should confirm that the new hostname resolves locally and externally to the IP address.

Example

```
admin:utils network host cer-191-p123
Local Resolution:
cer-191-p123.cisco.com resolves locally to 10.77.29.191 (CER-191-P123.cisco.com)

External Resolution:
cer-191-p123.cisco.com has address 10.77.29.191
```

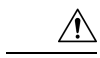
Pre-Change Setup

Perform all pre-change setup tasks to ensure that your system is prepared for a successful IP address, hostname, domain, or node name change. You must perform these tasks during a scheduled maintenance window.

You should perform the system health checks on your deployment before performing the pre-change setup.

Perform Pre-Change Setup Tasks for Cisco Emergency Responder Nodes

Perform the following pre-change setup tasks before you change the IP address or hostname. You must perform these tasks during a scheduled maintenance window. See the pre-change task list for more information.



Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Before you begin

Perform the system health checks on your deployment.

Procedure

Step 1 From Cisco Unified Communications Manager Administration on the first node, select **System > Server** and click **Find**. A list of all servers in the cluster displays. Retain this list of servers for future reference.

Ensure that you save an inventory of both the hostname and IP address of each node in your cluster.

Step 2 Run a manual Disaster Recovery System backup and ensure that all nodes and active services are backed up successfully. For more information, see the *Disaster Recovery System Administration Guide* for your release.

IP Address and Hostname Changes

The following sections provide important information on IP Address and Hostname Changes. You must read these sections before you change an IP address or Hostname.

Change IP Address and Hostname Task List

The following table lists the tasks to perform to change the IP address and hostname for Cisco Emergency Responder nodes.

Table 1: Change IP Address and Hostname Task List

Item	Task
1.	Perform the pre-change tasks and system health checks.
2.	Change the IP address or hostname for the node using either the Command Line Interface (CLI) or the Unified Operating System GUI.
3.	Perform the post-change tasks.

Change IP Address or Hostname Using Unified Operating System GUI

You can use Cisco Unified Operating System Administration to change the IP address or hostname for publisher and subscriber nodes that are defined by a hostname in your deployment. Unless otherwise stated, each step in this procedure applies to both publisher and subscriber nodes on Cisco Emergency Responder Server Group.

Before you begin

Perform the pre-change tasks and system health checks on your deployment.

Procedure

Step 1 From Cisco Unified Operating System Administration, select **Settings** > **IP** > **Ethernet**.

Step 2 Change the hostname, IP address, and if necessary, the default gateway.

Step 3 Click **Save**.

What to do next

Perform all applicable post-change tasks to ensure that your changes are properly implemented in your deployment.

Note Do not proceed if the new hostname does not resolve to the correct IP address. If your cluster is using CA-signed certificates, you will need to have them re-signed. Run the CTL client and update the CTL file if the Cisco Unified Communications Manager cluster security is operating in mixed mode.

Change IP Address or Hostname Using CLI

You can use the Command Line Interface (CLI) to change the IP address or hostname for publisher and subscriber nodes that are defined by a hostname in your deployment. Unless otherwise stated, each step in this procedure applies to both publisher and subscriber nodes on Cisco Emergency Responder Server Group.

Before you begin

Perform the pre-change tasks and system health checks on your deployment.

Procedure

Step 1 Log into the CLI of the node that you want to change.

Step 2 Enter **set network hostname**.

Step 3 Follow the prompts to change the hostname, IP address, or default gateway.

a) Enter the new hostname and press **Enter**.
b) Enter **Yes** if you also want to change the IP address; otherwise, go to Step 4.
c) Enter the new IP address.
d) Enter the subnet mask.
e) Enter the address of the gateway.

Step 4 Verify that all your input is correct and enter **yes** to start the process.

Step 5 Wait for all services to come up on the node where the change is applied.

Step 6 If the change is applied on Publisher and only Hostname is changed, restart Cisco Emergency Responder service on Publisher.

Step 7 If the change is applied on Publisher and IP address is also changed along with the Hostname; restart Cisco Emergency Responder service on both Publisher and Subscriber node.

Step 8 If the node that you have changed is a subscriber node, reboot the node.

What to do next

Perform all applicable post-change tasks to ensure that your changes are properly implemented in your deployment.

Note Do not proceed if the new hostname does not resolve to the correct IP address.

If your cluster is using CA-signed certificates, you will need to have them re-signed. Run the CTL client and update the CTL file if the Cisco Emergency Responder cluster security is operating in mixed mode.

Example CLI Output for Set Network Hostname: Changing Hostname Only of Publisher

The following code shows an example of the CLI Output for Set Network Hostname.

```
admin:set network hostname

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y

ctrl-c: To quit the input.



         ***   W A R N I N G   ***
Do not close this window without first canceling the command.

This command will automatically restart system services.
The command should not be issued during normal operating
hours.

======================================================
 Note: Please verify that the new hostname is a unique
       name across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
======================================================

Security Warning : This operation will regenerate
       all CUCM Certificates including any third party
       signed Certificates that have been uploaded.

Enter the hostname:: newHostName
Would you like to change the network ip address at this time [yes]:: no


Warning: Do not close this window until command finishes.


Hostname: newHostName

Do you want to continue [yes/no]? yes

calling 1 of 10 component notification script: acluster_healthcheck.sh
```

```
calling 2 of 10 component notification script: adns_verify.sh
No Primary DNS server defined
No Secondary DNS server defined
calling 3 of 10 component notification script: aetc_hosts_verify.sh
calling 4 of 10 component notification script: ahostname_callback.sh
Info(0): Processnode query returned using cer195pub123:
hostaddress
============
cer195pub123
updating cerserver table from:'cer195pub123', to: 'newHostName'
Rows: 1
updating cersystemparameters table from:'cer195pub123', to: 'newHostName'
Rows: 3
updating database, please wait 90 seconds
updating database, please wait 60 seconds
updating database, please wait 30 seconds
calling 5 of 10 component notification script: clm_notify_hostname.sh
Verifying update across cluster nodes...
Updating platformConfig.xml: cer195pub123 to newHostName
Updating platformConfig.xml: cer195pub123 to newHostName
Updating platformConfig.xml: cer195pub123 to newHostName
Updating processnode.xml: cer195pub123 to newHostName
\  Restarting Cluster Manager service... Please Wait


cluster update successfull
calling 6 of 10 component notification script: drf_notify_hostname_change.py
calling 7 of 10 component notification script: elm_client_reset_registration
calling 8 of 10 component notification script: idsLocalPrefsUpdateFile.sh
Going to trigger /usr/bin/python /usr/local/er/lib/dblupdatefiles-plugin.py
-f=newHostName,cer195pub123
calling 9 of 10 component notification script: regenerate_all_certs.sh
calling 10 of 10 component notification script: update_idsenv.sh

System services will restart in 1 minute
admin:
```

Example CLI Output for Set Network Hostname: Changing IP Address and Publisher Hostname

The following code shows an example of the CLI Output for Set Network Hostname.

```
admin:set network hostname

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y

ctrl-c: To quit the input.


         ***   W A R N I N G   ***
Do not close this window without first canceling the command.

This command will automatically restart system services.
The command should not be issued during normal operating
hours.

=====================================================
 Note: Please verify that the new hostname is a unique
       name across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
```

```
=====================================================

Security Warning : This operation will regenerate
       all CUCM Certificates including any third party
       signed Certificates that have been uploaded.

Enter the hostname:: newHostNameAndnewIPAddress
Would you like to change the network ip address at this time [yes]::


Warning: Do not close this window until command finishes.



ctrl-c: To quit the input.



           ***   W A R N I N G   ***
=====================================================
 Note: Please verify that the new ip address is unique
       across the cluster.
=====================================================

Enter the ip address:: 10.77.29.186
Enter the ip subnet mask:: 255.255.255.0
Enter the ip address of the gateway:: 10.77.29.1
Hostname:       newHostNameAndnewIPAddress
IP Address:     10.77.29.186
IP Subnet Mask: 255.255.255.0
Gateway:        10.77.29.1

Do you want to continue [yes/no]? yes

calling 1 of 6 component notification script: ahostname_callback.sh
Info(0): Processnode query returned using newHostName:
hostaddress
===========
newHostName
updating cerserver table from:'newHostName', to: 'newHostNameAndnewIPAddress'
Rows: 1
updating cersystemparameters table from:'newHostName', to: 'newHostNameAndnewIPAddress'
Rows: 3
updating database, please wait 90 seconds
updating database, please wait 60 seconds
updating database, please wait 30 seconds
calling 2 of 6 component notification script: clm_notify_hostname.sh
Verifying update across cluster nodes...
Updating platformConfig.xml: newHostName to newHostNameAndnewIPAddress
Updating platformConfig.xml: newHostName to newHostNameAndnewIPAddress
Updating platformConfig.xml: newHostName to newHostNameAndnewIPAddress
Updating processnode.xml: newHostName to newHostNameAndnewIPAddress
\  Restarting Cluster Manager service... Please Wait


cluster update successfull
calling 3 of 6 component notification script: drf_notify_hostname_change.py
calling 4 of 6 component notification script: idsLocalPrefsUpdateFile.sh
Going to trigger /usr/bin/python /usr/local/er/lib/dblupdatefiles-plugin.py
-f=newHostNameAndnewIPAddress,newHostName
calling 5 of 6 component notification script: regenerate_all_certs.sh
calling 6 of 6 component notification script: update_idsenv.sh
calling 1 of 3 component notification script: aaupdateip.sh
calling 2 of 3 component notification script: ahostname_callback.sh
```

```
Info(0): Processnode query returned =
name
================================================
10.77.29.195-AdminUpdateManager
10.77.29.195-SystemUpdateManager
updating server table from:'10.77.29.195', to: '10.77.29.186'
Rows: 1
Rows: 1
updating database, please wait 90 seconds
updating database, please wait 60 seconds
updating database, please wait 30 seconds
calling 3 of 3 component notification script: clm_notify_hostname.sh
Verifying update across cluster nodes...
Shutting down interface eth0:
```

Change IP Address Only

Do not use **set network hostname** CLI command to change IP Address only.

Command Syntax

set network ip eth0 ip-address ip-mask gate-way

Syntax Description

Parameters	Description
eth0	Specifies Ethernet interface 0.
ip-address	The IP address that you want assign.
ip-mask	The IP mask that you want to assign.
gate-way	The IP of default gate way to be assigned.

Example

Note For further information please refer the admin guide IP address change section.

```
admin:set network ip eth0 10.77.34.243 255.255.255.0 10.77.34.1

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y
           ***   W A R N I N G   ***
This command will restart system services
======================================================
 Note: Please verify that the new ip address is unique
       across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
======================================================
```

```
Continue (y/n)?y
calling 1 of 7 component notification script: aaupdateip.sh
calling 2 of 7 component notification script: acluster_healthcheck.sh
calling 3 of 7 component notification script: adns_verify.sh
Verifying 10.77.34.243 against primary DNS server 10.77.34.227 ...
Successfully verified against primary DNS server 10.77.34.227
IPADDR_RETURNED matches 10.77.34.243
calling 4 of 7 component notification script: aetc_hosts_verify.sh
calling 5 of 7 component notification script: ahostname_callback.sh
Info(0): Processnode query returned =
name
================================================
10.77.34.207-AdminUpdateManager
10.77.34.207-SystemUpdateManager
updating server table from:'10.77.34.207', to: '10.77.34.243'
Rows: 1
Rows: 1
updating database, please wait 90 seconds
updating database, please wait 60 seconds
updating database, please wait 30 seconds
calling 6 of 7 component notification script: clm_notify_hostname.sh
Verifying update across cluster nodes...
Shutting down interface eth0:
```

Post-Change Tasks and Verification

The following sections provide information on post-change tasks and verification. You must read these sections and perform these tasks to complete the IP Address and Hostname changes.

Post-Change Task List for Cisco Emergency Responder Nodes

The following table lists the tasks to perform after you have changed the IP address or hostname of the Cisco Emergency Responder nodes in your cluster.

Perform the tasks that apply to your deployment in the order in which they are presented in the task list. For details about system health checks or generating ITL certificates, see the related topics.

Table 2: Post-Change Task List for Cisco Emergency Responder Nodes

Item	Task
System health checks	
1.	Ensure that all servers in the cluster are up and available, and check for any active ServerDown alerts. **Note** ServerDown alerts in the Syslog are normal during the change process, but should not appear in the log after the change is done.
2.	Check the database replication status of all Cisco Emergency Responder nodes in the cluster to ensure that all servers are replicating database changes successfully.
3.	Check network connectivity and DNS server configuration on the node that was changed using the CLI command **utils diagnose module validate_network**.
Security enabled cluster tasks	

Item	Task
4.	For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the CTL file and then restart all nodes in the cluster before you perform the system health checks and other post-change tasks. For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, see the *Cisco Unified Communications Manager Security Guide* .
5.	If you enabled cluster security using Certificate Trust List (CTL) files and USB eTokens, you must regenerate the Initial Trust List (ITL) file and the certificates in the ITL. Skip this step if you have not enabled cluster security using Certificate Trust List (CTL) files and USB eTokens.
Post-change tasks	
6.	Run a manual DRS backup and ensure that all nodes and active services back up successfully. For more information, see the Disaster Recovery System Administration Guide for your release. **Note** You must run a manual DRS backup after you change the IP address of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.
7.	If you are using the integrated DHCP server that runs on Cisco Unified Communications Manager, update the DHCP server.

Perform Post-Change Tasks for Cisco Emergency Responder Nodes

Perform all post-change tasks to ensure that your changes are properly implemented in your deployment. Perform the tasks in the order in which they are presented in the task list.

Before you begin

Before you perform your post-changes tasks, you must:

- Perform all applicable system health checks to verify the changes that were made to your deployment.
- Perform the security enabled cluster tasks if cluster security is enabled for your deployment.

Procedure

Step 1 Run a manual DRS backup and ensure that all nodes and active services back up successfully. For more information, see the *Disaster Recovery System Administration Guide* for your release.

Note You must run a manual DRS backup after you change the IP address of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.

Step 2 If you are using the integrated DHCP server that runs on Cisco Unified Communications Manager, update the DHCP server.

Troubleshooting

The following sections provide information on troubleshooting an IP Address and Hostname change. Use this information to diagnose and resolve any issues.

Troubleshoot Cluster Authentication

You can troubleshoot cluster authentication issues on subscriber nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **show network eth0 [detail]** to verify network configuration.

Step 2 Enter **show network cluster** to verify the network cluster information.

- If the output displays incorrect publisher information, enter the **set network cluster publisher [hostname/IP address]** CLI command on the subscriber node to correct the information.
- If you are on a publisher node, and the show network cluster CLI command displays incorrect subscriber information, login to Cisco Emergency Responder Administration and choose **System** > **Server Settings** to check the output.
- If you are on a subscriber node and the show network cluster output displays incorrect publisher information, use the **set network cluster publisher [hostname | IP_address]** CLI command to change the publisher hostname or IP address.

Troubleshoot Database Replication

You can use the Command Line Interface (CLI) to troubleshoot database replication on the nodes in your cluster.

- Verify that database replication is in a correct state in the cluster.
- Repair and reestablish database replication for the nodes.
- Reset database replication.

For more information about these commands or using the CLI, see the *Command Line Interface Guide for Cisco Emergency Responder Administration Guide*.

Verify Database Replication

Use the Command Line Interface (CLI) to check the database replication status for all nodes in the cluster. Verify that the Replication STATE is shown as "Active" for both publisher and subscriber replication server.

Anything other than "Active" state (for example, "Dropped", "Connecting") means that there is a problem with database replication and that you need to reset replication for the node. See topics related to database replication examples for example output.

Procedure

Enter **utils dbreplication status** on the publisher and subscriber to check database replication on both the nodes in a Server Group.

Note If replication is not set up for the nodes in your cluster, you can reset database replication for the nodes using the CLI. For more information, see topics related to resetting database replication using the CLI

Example:

```
On Publisher

admin:utils dbreplication status

 -------------------- utils dbreplication status --------------------
Output is in file /var/log/active/er/trace/dbl/sdi/ReplicationStatus.2014_10_13_18_24_02.out

Please use "file view activelog er/trace/dbl/sdi/ReplicationStatus.2014_10_13_18_24_02.out
 " command to see the output
admin:file view activelog er/trace/dbl/sdi/ReplicationStatus.2014_10_13_18_24_02.out

Mon Oct 13 18:24:02 2014 main()  DEBUG:  -->
Mon Oct 13 18:24:02 2014 main()  DEBUG:  Replication cluster summary:
SERVER                 ID STATE    STATUS     QUEUE  CONNECTION CHANGED
------------------------------------------------------------------------
g_2_cer10_5_0_98000_9000    2 Active   Local           0
g_3_cer10_5_0_98000_9000    3 Active   Connected       0 Oct 13 17:31:15
Mon Oct 13 18:24:03 2014 main()  DEBUG:  <--

end of the file reached
options: q=quit, n=next, p=prev, b=begin, e=end (lines 1 - 7 of 7) :
admin:
On Subscriber:

admin:utils dbreplication status

 -------------------- utils dbreplication status --------------------
Output is in file /var/log/active/er/trace/dbl/sdi/ReplicationStatus.2014_10_13_18_33_14.out

Please use "file view activelog er/trace/dbl/sdi/ReplicationStatus.2014_10_13_18_33_14.out
 " command to see the output
admin:file view activelog er/trace/dbl/sdi/ReplicationStatus.2014_10_13_18_33_14.out

Mon Oct 13 18:33:14 2014 main()  DEBUG:  -->
Mon Oct 13 18:33:14 2014 main()  DEBUG:  Replication cluster summary:
SERVER                 ID STATE    STATUS     QUEUE  CONNECTION CHANGED
------------------------------------------------------------------------
g_2_cer10_5_0_98000_9000    2 Active   Connected       0 Oct 13 17:31:15
g_3_cer10_5_0_98000_9000    3 Active   Local           0
Mon Oct 13 18:33:15 2014 main()  DEBUG:  <--

end of the file reached
options: q=quit, n=next, p=prev, b=begin, e=end (lines 1 - 7 of 7) :
```

```
admin:
```

Repair Database Replication

Use the Command Line Interface (CLI) to repair database replication.

Procedure

Step 1 Enter **utils dbreplication repair all** on the Publisher to attempt to repair database replication.

Depending on the size of the database, it may take several minutes to repair database replication. Proceed to the next step to monitor the progress of database replication repair.

Example:

```
admin:utils dbreplication repair all
 -------------------- utils dbreplication repair --------------------
Logs for the repair of ~informix/.rhosts file is present in er/logs/repair-rhosts-1818.log
 file
/usr/local/er/db/informix/bin/cdr list server >>
/var/log/active/er/trace/dbl/sdi/ReplicationRepair.2014_10_13_18_38_07.out 2>&1
Output is in file er/trace/dbl/sdi/ReplicationRepair.2014_10_13_18_38_07.out

Please use "file view activelog er/trace/dbl/sdi/ReplicationRepair.2014_10_13_18_38_07.out
 " command to see the output
admin:
```

Step 2 View the ReplicationRepair file as mentioned in step 1 to check whether all tables are scanned and replicated properly. Any error will be reflected in this file.

If errors or mismatches are found, there may be a transient mismatch between nodes. Run the procedure to repair database replication again.

Note If, after several attempts to repair replication, mismatches or errors are being reported, try resetting the replication to resolve this issue.

Reset Database Replication

Reset database replication if replication is not set up for the nodes in your cluster. You can reset database replication using the command line interface (CLI).

Procedure

Step 1 Reset replication on nodes in your cluster. Do the following:

a) Enter **utils db replication reset all** on Publisher node in a CER Server Group.

b) Before you run this CLI command on the Publisher node, first run the command **utils dbreplication stop** on subscriber node, and then on the publisher node.

Step 2 After the command is executed successfully on Publisher node, restart subscriber node.

Troubleshoot Network

You can troubleshoot network issues on nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **show network eth0 [detail]** to verify network configuration.

Step 2 If any of the fields are missing, then reset the network interface.

a) Enter **set network status eth0 down**.

b) Enter **set network status eth0 up**.

Step 3 Verify the IP address, mask, and gateway. Ensure that these values are unique across the network.

Troubleshoot Network Time Protocol

The following sections discuss troubleshooting NTP issues on the Publisher and Subscriber nodes. Use this information to resolve any potential issues.

Troubleshoot NTP on Subscriber Nodes

You can troubleshoot Network Time Protocol (NTP) issues on subscriber nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **show network eth0 [detail]** to verify network configuration.

Step 2 Enter **utils ntp status** to verify NTP status.

Step 3 Enter **utils ntp restart** to Restart NTP.

Step 4 Enter **show network cluster** to verify the network cluster.

If the output displays incorrect publisher information, use the **set network cluster publisher [hostname/IP_address]** CLI command to reset the publisher.

Troubleshoot NTP on Publisher Nodes

You can troubleshoot Network Time Protocol (NTP) issues on publisher nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **show network eth0 [detail]** to verify network configuration.

Step 2 Enter **utils ntp status** to verify NTP status.

Step 3 Enter **utils ntp restart** to Restart NTP.

Step 4 Enter **utils ntp server list** to verify NTP servers.

To add or delete an NTP server, use the **utils ntp server [add/delete]** CLI command.

Change IP Address and Hostname