Troubleshooting

Troubleshooting

Restarting Sequence

Whenever you have formed, connected, upgraded, or changed a cluster, you should check whether any peers need restarting. Sometimes you will need to restart only one peer, typically if you've made a peer-specific configuration change.

When you're working with the cluster configuration, you sometimes need to restart more than one peer. In this case, you should always restart in the following sequence:

1. Restart the primary peer, and wait for it to be accessible via web interface.

2. Check cluster replication status on the primary and status of all peers. Wait a few minutes, refreshing the peer's web interfaces occasionally.

3. Restart other peers, if required, one at a time. Each time, wait a few minutes after it is accessible and check its replication status.

Check Replication Status

You may need to wait about 5 minutes after making clustering changes before the Expressway peers report successful status.

1. Go to **System** > **Clustering** on each peer and check that the cluster database status reports as Active.

   If there is a failure status, refresh the browser first. If the status is still not Active, check the alarms.

Force Refresh in Cisco TMS

If you're using Cisco TMS, check that Cisco TMS has all the correct settings for the cluster by forcing a refresh as follows:

Procedure

Step 1	On Cisco TMS, go to **Systems** > **Navigator**.
Step 2	Find and click on the name of the Expressway.
Step 3	Select the **Settings** tab.
Step 4	Click **Force Refresh**.
Step 5	Repeat for all Expressway peers in the cluster (including the primary Expressway).

Expressway Alarms and Warnings

Cluster name not configured: if FindMe or clustering are in use a cluster name must be defined

Ensure that the same cluster name is configured on each Expressway in the cluster.

The **Cluster name** should be the routable Fully Qualified Domain Name used in SRV records that address this Expressway cluster, for example "cluster1.example.com". (See Cluster Name and DNS SRV Records).

Cluster replication error: (details) manual synchronization of configuration is required

This may be:

- "Cluster replication error: manual synchronization of configuration is required"

- "Cluster replication error: cannot find primary or this subordinate's peer configuration file, manual synchronization of configuration is required"

- "Cluster replication error: configuration primary ID is inconsistent, manual synchronization of configuration is required"

- "Cluster replication error: this peer's configuration conflicts with the primary's configuration, manual synchronization of configuration is required"

If a subordinate Expressway reports an alarm: "Cluster replication error – <details> synchronization of configuration"

On that subordinate Expressway:

1. Log in as admin on an SSH or other CLI interface.

2. At the command prompt type:

```
xcommand ForceConfigUpdate
```

This will delete the subordinate Expressway configuration and then force it to update its configuration from the primary Expressway.

⚠️

Caution Only use this command if the configuration on the primary Expressway is known to be in a good state. We recommend that you take a backup before running this command.

Cluster replication error persists after ForceConfigUpdate

In X8.11 we introduced a unique encryption key per cluster peer. Also, in some upgrade cases, for example, if peers are upgraded in the wrong order, subordinate peers may not synchronize with the primary. These two issues compound each other, allowing peers to be in a state where they cannot decrypt the configuration from the primary.

The symptom of this is that the Cluster replication alarm persists after you tried `xcommand forceconfigupdate` on a subordinate peer. This is probably after a recent upgrade to X8.11 on the primary peer.

You can avoid the problem by always upgrading the primary first, but if you have got this persistent error, you can resolve it as follows:

1. Sign in to the primary peer and check that it is in a good state.

2. Ensure that the clustering configuration shows this peer to be the primary.

3. Upgrade the primary again, using the same package that you originally used to upgrade.

The replication alarm clears after the primary peer has upgraded and rebooted. This normally happens within ten minutes after reboot, but could be up to twenty minutes after reboot.

Cluster replication error: the NTP server is unreachable

Configure an accessible NTP server on the Expressway **System** > **Time** page.

Cluster replication error: the local Expressway does not appear in the list of peers

Check and correct the list of peers for this Expressway on the primary Expressway, and copy to all other Expressway peers (**System** > **Clustering**).

Cluster replication error: automatic replication of configuration has been temporarily disabled because an upgrade is in progress

Wait until the upgrade has completed.

Invalid clustering configuration: H.323 mode must be turned On - clustering uses H.323 communications between peers

Ensure that H.323 mode is on (see **Configuration** > **Protocols** > **H.323**).

Expressway database failure: Please contact your Cisco support representative

The support representative will help you work through the following steps:

1. Take a system snapshot and provide it to your support representative.

2. Remove the Expressway from the cluster using: Remove a Live Peer From a Cluster (Permanently).

3. Restore that Expressway's database by restoring a backup taken on that Expressway previously.

4. Add the Expressway back to the cluster using Add a Peer to a Cluster.

A second method is possible if the database does not recover:

1. Take a system snapshot and provide it to TAC.

2. Remove the Expressway from the cluster using: Remove a Live Peer From a Cluster (Permanently).

3. Log in as root and run `clusterdb_destroy_and_purge_data.sh`

4. Restore that Expressway's database by restoring a backup taken on that Expressway previously.

5. Add the Expressway back to the cluster using Add a Peer to a Cluster.

> **Note** `clusterdb_destroy_and_purge_data.sh` is as dangerous as it sounds — only use this command in conjunction with instructions from your support representative.

Cisco TMS Warnings

Cisco TMS Cluster Diagnostics

If Cisco TMS cluster diagnostics reports a difference in configuration on Expressway peers, it is comparing the output of `https://<ip address>/alternatesconfiguration.xml` for each Expressway.

To manually check the differences, on a Unix / Linux system, run:

```
wget --user=admin --password=<password> --no-check-certificate https://<IP or FQDN of
Expressway>/alternatesconfiguration.xml
```

for each of the Expressway peers, then use diff to check for differences.

Conference Factory Template Does Not Replicate

This is by design; the Conference Factory %% value is NOT shared between cluster peers and the Conference Factory application configuration is NOT replicated across a cluster.

See Impact of Clustering in Other Expressway Applications.

Expressway's External Manager Protocol Keeps Getting Set to HTTPS

Cisco TMS can be configured to force specific management settings on connected systems. This includes ensuring that a Expressway uses HTTPS for feedback. If enabled, Cisco TMS will (on a time period defined by Cisco TMS) re-configure the Expressway's **System** > **External Manager Protocol** to *HTTPS*.

If HTTPS must be used for Expressway to supply feedback to Cisco TMS, see Add the Expressway to Cisco TMS for information about how to set up certificates.

Cisco TMS will force HTTPS on Expressway if:

- **TMS Services** > **Enforce Management Settings on Systems** = *On* (**Administrative Tools** > **Configuration** > **Network Settings**)

  and

- **Secure-Only Device Communication** > **Secure-Only Device Communication** = *On* (**Administrative Tools** > **Configuration** > **Network Settings**)

Set **Enforce Management Settings on Systems** to *Off* if Cisco TMS does not need to force the management settings.

Set **Secure-Only Device Communication** to *Off* if it is unnecessary for Expressway to provide feedback to Cisco TMS using HTTPS (if HTTP is sufficient).