Migration from Legacy Network to HTTPS Network

Migration from Legacy Network to HTTPS Network

Migration from Legacy Network to HTTPS Network

In Cisco Unity Connection two or more Unity Connection servers or clusters can be connected through HTTPS links in a hub-spoke topology to form a single site network, referred to as an HTTPS Unity Connection network.

Migration from legacy network to HTTPS network can be done using a flash-cut approach which includes unjoining the existing network and then joining the locations in a pre-decided network topology.

A downtime window is required for the migration activity, which varies depending on the number of locations and the directory size; hence it should be planned during off-hours or over the weekend. Since legacy links are not supported in HTTPS networking, the entire network should collectively be migrated to the HTTPS network.

Prerequisites for Migration from Legacy to HTTPS Network

Before proceeding with the migration activity, ensure the following prerequisites have been met on each server that joins in the HTTPS network (for clusters, verify these prerequisites for the publisher server):

• For a Unity Connection site, the directory replication is working fine and none of the locations have stalled replication. Unity Connection SMTP server and Connection Digital Networking Replication Agent services are up and running. Visit https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/serv_administration/b_12xcucservag/b_12xcucservag_chapter_0100.html for more details on description and management of Cisco Unity Connection Services.

• All locations in the network are in synchronization with each other.

• For Intrasite links, this can be determined as mentioned in section " Checking Replication Status Within a Site " section of the "Setting Up Networking between Cisco Unity Connection Servers" chapter of the *Networking Guide for Cisco Unity Connection, Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/networking/guide/b_12xcucnetx.html.

- For Intersite links, see section "Checking the Status of Synchronization Between Unity Connection Sites and Configuring Task Schedules " of the "Setting Up Networking between Cisco Unity Connection Servers" chapter of the *Networking Guide for Cisco Unity Connection, Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/networking/guide/b_12xcucnetx.html. Verify that the latest synchronization task has completed without any errors.

- Upgrade all the locations to connection release 12.x. The HTTPS networking feature is available only from release 12.x onwards. See https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/install_upgrade/guide/b_12xcuciumg/b_12xcuciumg_chapter_00.html for upgrading a network location to 12.x version.

- After upgrade, take a data backup for all locations in the legacy network. See *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/install_upgrade/guide/b_12xcuciumg.html. which provides an overview of the Disaster Recovery System, describes how to use the Disaster Recovery System, and provides procedures for completing various backup-related tasks and restore-related tasks.

- The network administrator needs to decide the HTTPS network topology and arrangement of Unity Connection servers prior to the migration of the network. See section "Deciding the Network Topology" at Setting Up an HTTPS Network

Task List to Migrate from Legacy Network to HTTPS Network using Flash Cut Approach

After ensuring that the conditions specified in Prerequisites for Migration from Legacy to HTTPS Network section are met, proceed with the following steps to migrate the network:

Step 1 On each Unity Connection location in the network, take a backup of distribution lists, both public and private, and distribution list members that are homed at that location. The Distribution List Syncher tool can be used for this purpose. For more information on the tool visit:
http://www.ciscounitytools.com/Applications/CxN/DistributionListBuilderCsv/DistributionListBuilderCsv.html.

Step 2 Schedule the task "Update Database Statistics" to run every 2 hours. Visit **Tools** > **Task Management** > **help** > **This Page** for details regarding task definitions, task definition basics and task schedules.

Step 3 Unjoin the locations in the network. It is recommended to unjoin only two locations at a time from the network, since unjoining more locations increases the SMTP traffic during replication and can halt replication.

See section Removing a Location From a Unity Connection Site of https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/networking/guide/b_12xcucnetx/b_12xcucnetx_chapter_0101.html for steps to unjoin an Intrasite network. It is also recommended that the Intrasite links be removed using Remove Self from Site option.For more information visit **Networking** > **Legacy Links** > **Intrasite Links** > **Help** > **This Page**.

Also see section Removing an Intersite Link Between Two Cisco Unity Connection 12.x Sites at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/networking/guide/b_12xcucnetx/b_12xcucnetx_chapter_0101.html for steps to unjoin an Intersite network.

Step 4 Schedule the "Update Database Statistics" task to run at its default time. Visit **Tools** > **Task Management** > **help** > **This Page** for details regarding task definitions, task definition basics and task schedules.

Step 5 Take a DRS backup of all the locations. See section "About Disaster Recovery System" of Backing Up and Restoring Cisco Unity Connection Components chapter in *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 12.x,* available at

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/install_upgrade/guide/b_12xcuciumg.html.which provides an overview of the Disaster Recovery System, describes how to use the Disaster Recovery System, and provides procedures for completing various backup-related tasks and restore-related tasks.

Step 6   Join the locations in HTTPS network as per the topology decided by the network administrator and allow the directory replication to complete. See Setting Up an HTTPS Network for details regarding joining locations in HTTPS network and verifying the synchronization status.

Step 7   In an HTTPS network, by default the system distribution lists and its members are not synchronized between the locations in the network. To enable the synchronization of distribution lists and its members, of a particular Unity Connection location, you need to check the Include distribution lists and membership when synchronizing directory data check box on the Edit HTTPS Link page of the corresponding location.

It is recommended that synchronization of distribution list should be initiated after the completion of first directory synchronization cycle.

If you enable the Include distribution lists and membership when synchronizing directory data check box on one location in the network, it is recommended to check the check box on all the locations in the network.

Caution   When you enable system distribution list synchronization, you cannot disable it afterwards, except by removing and recreating the HTTPS link.

Allow the directory synchronization to complete after enabling the checkbox on the locations.

Step 8   Once the directory replication is complete, start restoring the public and private distribution lists from the backup taken in step Step 1. The Distribution List Syncher tool can be used for this purpose. For more information on the tool see: http://www.ciscounitytools.com/Applications/CxN/DistributionListBuilderCsv/DistributionListBuilderCsv.html .

Step 9   After restoring distribution lists and distribution list members from the backup, allow the directory replication to complete between the locations.