# Creating a Multi-data Center (MDC) System



# Creating a Multi-data Center (MDC) System

## About Multi-data Centers

The Multi-data Center (MDC) licensed feature is available in version 2.5 and higher. It allows two CWMS systems to be joined into a single MDC system. One license must be purchased for each CWMS data center in an MDC system. MDC licenses should be purchased before you attempt to deploy MDC. (A system with a single data center does not need a feature license.) MDC licenses are further described in About MDC Licenses.

The meeting client uses the Round Trip Time (RTT) to determine on which data center to start meeting. (This is an automated process and cannot be configured by the host or the administrator.)

Load Balancing is not configurable; it is automatic and built into the system. Any Load Balancer configured as separate machine is not supported.

Network requirements between data centers can be found in the "Network Requirements for Multi-data Center" chapter of the CWMS Planning Guide at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html.

### Advantages of a Multi-data Center System

The advantages include:

- End user access to all data centers by using one URL and one set of phone numbers; the existence of MDC is transparent to end users.
- Host licenses, recordings, and related management data migrate freely between joined data centers.
- Users can dial into meetings without geographic restrictions; attend meetings by dialing local phone numbers.
- Data centers can (optionally) be located in different geographic areas.
- Zero-downtime during some planned maintenance events, when the data centers can be running different CWMS 2.5 *update* versions. Consult the release notes at http://www.cisco.com/c/en/us/support/

conferencing/webex-meetings-server/products-release-notes-list.html to determine which CWMS versions can run simultaneously.

Occasionally, data centers in an MDC system can be running different *update* versions. Consult the release notes at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-release-notes-list.html to determine which CWMS versions can run simultaneously.

- A disaster recovery environment that is transparent to users. If one data center fails for any reason, the other data center supports users.

Although in an MDC environment the data centers are all running CWMS and considered peers, for the purpose of describing the process for joining data centers in a system, the relationship between data centers are considered *primary* and *secondary*. Before the Join, the primary data center supports the *system* you want to retain, and shall be the location of the license manager. The secondary data center becomes part of the MDC system. The distinction is important especially if you are joining data centers that have been actively supporting users. User information and content are deleted from the secondary data center.

**Note** There is redundancy, but no increase in capacity when a data center is added to an MDC system. If a 2000-port data center is added to an MDC system supported by a 2000-port data center the resulting system is a 2000-port MDC.

If you are joining a new, secondary CWMS system data center that has no user data to an MDC system, continue to Preparing an MDC System to Receive Data Center Join Requests, on page 5.

If you are joining an active, secondary CWMS system data center that includes user data to an MDC system, continue to Preparing to Join an Active CWMS Data Center to a MDC System, on page 3.

### Blocking Mode

Each data center polls its components for their status every 5 seconds. Under certain failure conditions a data center automatically turns on Blocking Mode to prevent end users from accessing a data center with failed components, allowing time for the system to attempt to fix itself. In an MDC environment, user activity transparently fails over to the active data center. Once the components of the data center in Blocking Mode are again operational, the data center exits Blocking Mode. Email notifications are sent to administrators when a data center goes into or recovers from Blocking Mode.

Blocking Mode ON conditions are triggered when all the following are true:

- One or more of the telephony components or data base replication fails.
- The condition has existed for 5 minutes or more.
- Another data center in the MDC system is operational.

End-user access to a data center in Blocking Mode is prevented; all user activity is redirected to the active data center. Administrators can access the administration site on the blocked data center to monitor its condition and to troubleshoot issues.

Blocking Mode OFF conditions are automatic and are triggered by all of the components returning to a good state. Access by end-users is restored and the data center returns to polling its components every 5 seconds.

# Preparing to Join an Active CWMS Data Center to a MDC System

**Important** Joining CWMS data centers requires the use of RSA self-signed certificates. Before you begin the join, ensure that you remove Certificate Authority (CA) certificates from both data centers.

When you join a secondary CWMS system data center that has been in service to users, it has acquired or been configured with user data that might be lost when it is joined to a Multi-data Center (MDC). In a Single-data Center environment, one CWMS data center serves the user community. When a MDC system is desired, typically a new CWMS data center is created and joined to the MDC system before that data center is put it into service and therefore, there is no user information, licenses, or configuration information of value to retain on what will become the secondary data center during the Join. However, if you are joining two active data centers, user content is overwritten or inaccessible:

- All global data is overwritten. (Configuration parameters local to the data center are preserved.)
- User information, scheduled meetings, reports, and related emails that was on the secondary data center is deleted.
- Meeting recordings are inaccessible to users. The recordings remain intact on the NAS, but they cannot be accessed or recovered by users. (See Preserving Recordings before Joining a MDC System, on page 4.)
- Host licenses are lost, but Permanent Host licenses that were hosted on the secondary data center can be recovered by re-hosting them on the MDC system. If the primary data center is removed from the system, the licenses must be re-hosted on another data center running License Manager.

  If the primary data center goes off-line for any reason, it must be brought back online before host licenses can be modified. If the managing data center cannot be recovered, surviving data centers go into a grace mode for 180 days. To recover, Permanent Host licenses must be re-hosted before the grace period ends. (See Re-hosting Licenses.) If the licenses are not re-hosted before the grace period ends, the system is put into Maintenance Mode until the licenses are re-hosted.
- The user-to-host license associations on an active secondary data center are lost when data centers are joined. Users that were hosts on an active secondary data center can recover their licenses simply by hosting meetings on the joined system or an administrator can manually assign host licenses from the data center managing the licenses.

The following information on secondary data centers is retained after a join:

- System-specific configurations, such as Cisco Unified Call Manager (CUCM).
- Language settings, such as IVR language settings.
- Audio settings.
- Blast Dial information.

## Preserving CWMS Data on a Secondary Data Center Before a Join

The CWMS data on a secondary data center being joined to a MDC system is overwritten or rendered inaccessible. If you are joining a CWMS data center that has not been put into service, there is no meaningful

data to preserve and you can continue to Preparing an MDC System to Receive Data Center Join Requests, on page 5. Otherwise, consider preserving critical data.

When a secondary data center joins a MDC system, that data center loses:

- User-Host license associations
- Host licenses (that can be recovered by re-hosting them on the MDC systemRe-hosting Licenses after a Major System Modification)
- Scheduled meetings (that must be manually rescheduled on the MDC system)
- Meeting recordings that can be preserved by:
  - Asking users to download and retain recordings locally.
  - Archived for retrieval by a system administrator.
  - Both. (Recommended)

Meeting recordings "live" on the NFS, so they are not lost; they are not accessible to users from CWMS.

## Preserving Recordings before Joining a MDC System

Under the `NFS:/nbr` directory are the `Recording`, `nfskeepalive`, and `Snapshot` directories. To archive the files, copy `NFS1:/nbr/1/*` to `NFS2:/nbr/1`.

**Note** This procedure is provided as an example. The process for your system might vary.

For the purposes of the example steps, assume the NFS is on DC1 and named `sanjose-nfs:/cisco/cwms` and the NFS on DC2 is named `rtp-nfs:/cisco/cwms`.

### Before You Begin

- Access to a Linux machine with root access to the NFS. (Any flavor will do, Redhat, CentOS, and so forth.)

- If the NFS has an IP-based filtering or access control for mounting, then add the Linux host IP to the access list.

**Step 1** cd/tmp

**Step 2** Create a new temporary directory that will be used to mount the NFS of DC1. `mkdir nfs-dc1`.

**Step 3** Create a new temporary directory that will be used to mount the NFS of DC2 : `mkdir nfs-dc2`.

**Step 4** Mount DC1 NFS to `/tmp/nfs-dc1` : `mount -t nfs -o vers=3,rw,soft,timeo=400` *`sanjose-nfs:/cisco/cwms`* **`/tmp/nfs-dc1/`**

**Step 5** Mount DC2 NFS to `/tmp/nfs-dc2` : `mount -t nfs -o vers=3,rw,soft,timeo=400` *`rtp-nfs:/cisco/cwms`* **`/tmp/nfs-dc2/`**.

**Step 6** Synchronize the recordings : `rsync -av --exclude='*Snapshot*/' nfs-dc1/ nfs-dc2`.

**Step 7** Unmount the DC1 NFS : `umount nfs-dc1`.

**Step 8** Unmount the DC2 NFS : `umount nfs-dc2`.

**Step 9** Delete the DC1 NFS temporary mount directory : `rm -r nfs-dc1`.

**Step 10** Delete the DC2 NFS temporary mount directory : `rm -r nfs-dc2`.

# Preparing an MDC System to Receive Data Center Join Requests

Data centers can be joined and managed as a single system. This procedure describes how to prepare the *primary* data center that is already servicing the *system* to receive Join requests from the *secondary* data center:

### Before You Begin

The following is a list of tasks that a system administrator must complete to ensure that joining a data center to a system is successful.

1. Remove Certificate Authority (CA) certificates from both data centers. Joining CWMS data centers requires the use of RSA self-signed certificates.
2. Verify that all data centers are running the same CWMS software version.
3. Verify that all data centers are running the same software types. For example, verify that all data centers are Audio Encrypted -AE or Audio Unencrypted -AU. (Systems cannot be converted from one type of audio encryption to the other; a new system must be created.)
4. Verify that all data centers are the same system size.
5. Network Time Protocol (NTP) is required for all data centers, and all data centers must be on the same NTP time.
6. All virtual machine hosts must be configured with NTP servers.
7. NTP servers must be reachable from the virtual machine hosts. (Errors might occur if the DNS or firewall does not pass NTP or if the wrong NTP server configured.)
8. Install the Multi-data Center (MDC) licenses (two minimum) on the primary data center that is running the license manager.

9 All data centers in the system must have Internet Reverse Proxy (IRP) enabled or disabled. There cannot be a mismatch. After the Join, IRP can be added to or removed from any data center such that all data centers are configured the same way regarding IRP.

10 None of the data centers are running High Availability (HA). (See Removing High Availability from a System.)

11 Verify that storage is configured on both data centers or none of the data centers. If storage is configured, the data centers should use storage on different servers or at least different folders.

12 Verify that all data centers are using the same authentication mode. The authentication mode can be LDAP, SSO, or default mode.

13 Verify that the DNS has entries for all Local URLs, all Common URLs, and all hostnames. The Administration Common URL must be associated with only one IP address when the Join is executed. The WebEx Common URL must be associated with only one IP address when the Join is executed. After the data center is joined to a system, the common URL should be returning two IP addresses.

14 Verify the CUCM transports on both data centers use the same protocol. The transport protocol can be TCP, UDP, or TLS.

**Step 1** Notify users on the secondary system of the Join. If the secondary data center has not been a part of any active system, skip this step. If this data center is supporting an active system, see Preparing to Join an Active CWMS Data Center to a MDC System, on page 3.
User data, scheduled meetings, and access to meeting recordings on the secondary data center is lost when data centers are joined. Before you send a Join request from the secondary data center, notify all users that if they want to preserve any meeting recordings, they should download the recordings to their local PCs.

**Step 2** Select **Data Centers** > **Add Data Center** > **Prepare System for Join**

**Step 3** Enter:

- Local Site URL—User site URL that allows users to schedule, attend, or host meetings. When the network is not configured with split-horizon DNS (the most common configuration), this URL resolves to the public VIP address of this system for all users. When the network is configured with split-horizon DNS, this URL resolves to the private VIP address of this system for internal users and to the public VIP address of this system for external users.
- Local Administration URL—System administration URL that resolves to the private VIP address for this data center.
- Local Data Center Name—Identifies the primary data center on the local system.

**Step 4** Download the certificate that will be used to Join the systems.
The certificate from the primary data center must be uploaded to a secondary data center prior to the join. Certificates are modified by the system, so it is best not to try to reuse old certificates to accomplish a join.

**Note** When using Safari, the downloaded certificate is saved as `CAcert.pem.txt`. This is the default behavior of the Safari browser. To restore the `.pem` extension (before uploading the certificate), delete the `.txt` string.

**Step 5** Select **Done**.

**Step 6** Sign in to the secondary data center and send a Join request from that data center. See Joining a Data Center to a Multi-Data Center System, on page 7 for instructions.

# Joining a Data Center to a Multi-Data Center System

The Join request is sent from a *secondary* data center to the *primary* data center the data center supporting the CWMS Multi-data Center (MDC) system. After the join, the primary data center retains its data and access to meeting recordings. All meeting information and recordings on the secondary data center are rendered inaccessible. The MDC feature licenses and Permanent Host licenses are typically hosted and managed on the primary data center. There is no trial period for an MDC system; MDC licenses must be loaded on the primary data center prior to the Join. Without an available MDC license on the primary data center, a secondary data center cannot join a system.

**Note** When joining data centers, the primary data center certificates are updated. The new certificates are self-signed and automatically regenerated to include the new URLs from the secondary data center. This mismatch causes a certificate warning in the browser when you access the primary data center or the MDC Administration site. Accept the warnings and follow the standard procedure to update the system certificates. (See Managing Certificates.)

**Note** *When joining data centers that use languages other than English*, there is **always** a brief period during the Join operation when the task list appears in English. Error messages might also appear in multiple languages during a Join. (The balance of the text on the page appears in the original language.)

When the **Database tables are synchronized** task is launched, the expected task list language behavior is:

- If the Administrator account is hosted on all data centers and they are configured with the same language settings, the task list displays in English during the **Database tables are synchronized** task. After the tables are synchronized, the task names return to the language of the Administrator.
- If the Administrator account is hosted on the primary data center, and that administrator has an account on a data center that is joining the system and that data center is set to a different language than the primary data center, the task list displays in English while the database tables are synchronizing. After synchronization, the task list switches to the language the administrator set on the primary data center.
- If the Administrator account is hosted solely on the secondary data center joining the system, and the Administrator does not have an account on the primary data center that will remain after the Join, the task list displays in English while the database tables are synchronizing. Once the system finishes synchronization, there is no further language change and no **Done** button. To continue, the administrator must:

  1. Close the current browser window.
  2. Open a new window by using the local administration URL of the secondary data center.
  3. Sign in by using an Administrator account on the primary data center.
  4. Select **Data Centers** > **Add Data Center** and verify the status.

### Before You Begin

Network Time Protocol (NTP) must be configured as follows:

- NTP is required for all data centers and all data centers must be on the same NTP time.
- All virtual machine hosts must be configured with NTP servers.
- NTP servers must be reachable from the virtual machine hosts. (Errors might occur if the DNS or firewall does not pass NTP or if the wrong NTP server configured.)

If this data center is supporting an active system, Host licenses supported on this data center are removed. These Host licenses can be re-hosted on the data center hosting the License Manager. (See Re-hosting Licenses.) We recommend that you save a license request from this data center before you start the join in case you later need help from TAC to locate your licenses.

**Important** Joining CWMS data centers requires the use of RSA self-signed certificates. Before you begin the join, ensure that you remove Certificate Authority (CA) certificates from both data centers.

TLS 1.0 is marked as **Medium Vulnerability** by a PCI Vulnerability Scanning vendor. After the data center has joined the MDC, other certificates can be added to the system. See www.nist.gov/manuscript-publication-search.cfm?pub_id=915295 and www.tenable.com/blog/pci-ssc-announces-the-end-of-ssl-usage-for-the-payment-card-industry.

**Step 1** To send a request to join an MDC system from a secondary data center, select **Data Centers** > **Add Data Center** > **Join Systems**.

**Step 2** Enter:

- **Remote System Certificate—**Upload the System Certificate downloaded from the other data center during the "Preparing an MDC System to Receive Data Center Join Requests, on page 5" process.

  **Note** When using Safari, the downloaded certificate is saved as `CAcert.pem.txt`. This is the default behavior of the Safari browser. To restore the `.pem` extension (before uploading the certificate), delete the `.txt` string.

- **Remote Common Administration URL—**System administration URL that resolves to the private VIP address of the data center that you prepared to be joined.
- **Remote Administration Email—**Email address used for accessing the data center you are joining.
- **Remote Administrator Password—**Password that allows administrative access to the data center you prepared for the Join.
- **Local Data Center Name—**Identifies the secondary data center on the local system.

**Step 3** Select **Continue**.
The Join Data Center task list displays.

**Note** During the **Database tables are synchronized** task, all the users in the secondary data center are deleted and users listed on the primary data center are replicated over to the secondary data center. The system cannot get the administrator's language (as there are no users on DC2) and the interface defaults to displaying in English.

If the administrator of the secondary data center also exists on the primary data center, then after the administrator signs into the secondary data center, the system displays the administrator's language (unless the language configured on the primary data center for that administrator is a different language than what is configured on the secondary data center).

If the administrator of the secondary data center also exists on the primary data center (or there is an error in the database synchronization), then the system displays in English.

**Step 4** Take all data centers in the MDC system out of Maintenance Mode.

### What to Do Next

**Add the Pointers to the DNS Server**

- **Common site URL—**Public VIP address for each data center.
- **Common Administration URL—**Private VIP address of both data centers.
- **Local Site URL** (of a data center)**—**Public VIP address of that data center.
- **Local Site URL** (of the other data center)**—**Public VIP address of that data center.
- **Local Administration Site URL** (of a data center)**—**Private VIP address of that data center.
- **Local Administration Site URL** (of the other data center)**—**Private VIP address of that data center.

**Modify the Audio Access Numbers and Service Language**

The audio access number and service language configured on the primary data center are configured as the global access number and service language, replacing the original access number and service language configuration. If necessary, go to global configuration and adjust the access numbers and service language appropriately. (See Modifying Audio Settings.)

# Disaster Recovery in a Multi-data Center Environment

In a Multi-data Center (MDC) environment where one data center has failed due to a hardware or system issue, we recommend replacing the failed data center by creating a new data center and joining that data center to the system. (See also Disaster Recovery by Using the Storage Server). The replacement data center is quickly populated with the user information. If the License Server is on the failed data center, the MDC and user licenses must be re-hosted (see Re-hosting Licenses) on the replacement data center.

The remaining data center supports the system as long as it is up. However, the system does not have any redundancy in this scenario.

If the Data Base node of one data center goes down, data changes happening in the other data center are queued up. This queued data is synced when the failed data center comes up or when a replacement data center is joined.

If the queue grows beyond the limit, the data center stops queuing to prevent disk from becoming full and thus risking its own functionality. If the queue has exceeded the limit, the MDC does not attempt to synchronize data, even if the failed data center comes up; the system will no longer be an MDC from that point on.

Proper email notifications are sent out when failure is anticipated.

**Step 1** Sign on to the Administration site of the surviving data center.

**Step 2** Remove the failed data center from the system.
(See Removing a Data Center, on page 10).

**Step 3** Create a new data center to replace the failed data center.
The version of the replacement data center should match the version of the surviving data center.

**Step 4** Complete the local configurations, such as CUCM, SNMP, and so forth, matching the failed data center.

**Step 5** Prepare the surviving data center in the system to receive Join requests.
(See Preparing an MDC System to Receive Data Center Join Requests, on page 5).

**Step 6** Join the new data center to the system.
(See Joining a Data Center to a Multi-Data Center System, on page 7).

The data from the surviving data center is replicated on the new data center.

**Step 7** Update the DNS with the new URL and IP address information.

# Removing a Data Center

When a data center is removed from a Multi-data Center (MDC) system, all CWMS settings are removed. Parameters that applied to the removed data center are deleted from the surviving data center.

**Note** In a Multi-data Center (MDC) environment the License Manager is running on only one data center; it cannot run on more than one data center. If you remove the data center that is hosting the License Manager, you have 90 days to configure the License Manager on another data center and re-host the licenses. (See Register Licenses to be Re-hosted.)

### Before You Begin

Make a backup of the system and the data center to be removed.

Remove all the DNS and Communications Manager entries.

**Step 1** Power-off the virtual machines for the data center being removed.

**Step 2** Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

**Step 3** Select **Data Centers**.
The **Data Centers** window appears.

**Step 4** (Optional) Verify that the data center is unreachable.

You can verify this manually or you can begin the process of removing the data center and let CWMS check availability. If the data center can be pinged, the remove process does not proceed, and an error message appears.

**Step 5** To send a request to remove a data center from a MDC system, select **Remove** in the **Action** column.
If the data center being removed is hosting the License Manager, a warning appears. There is also a warning that DNS changes are required.

The primary data center is put into Maintenance Mode and the **Remove Data Center** window appears showing the progress of the action.

**Step 6** Select **Continue**

**Step 7** When all tasks are green, select **Done**.
The data center is removed and you are returned to the **Data Centers** window.

**Step 8** Verify that the data center was removed.
URLs for system access change and system only retains the global URLs.

**Step 9** Remove all DNS entries for the removed data center and map the Public and Private virtual IP addresses of the surviving data center to the global URLs.

**Step 10** Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

**Step 11** (Optional) If you removed the data center that hosts the License Manager, re-host the License Manager and licenses on the surviving data center.