Cisco TMS Server Redundancy

Configuration Guide

D14570.02

December 2010

Contents

Figures

Revision Notes

November 2010	▸ Rebranded with Cisco Systems.
September 2010	▸ Applied Cisco template and Cisco product names
Rev 2.1.1	▸ Fixed Bookmarks in PDF Output.
Rev 2.1	▸ Added Validation Key requirements. ▸ Corrected viewstate comments. ▸ Added sticky connection recommendation for NLBs. ▸ Minor formatting changes. ▸ Updated Cisco TMS version references to 11.7.
October 2009	▸ Updated template. ▸ New document number. (Old number: D50396).

Introduction

The Cisco TelePresence Management Suite (Cisco TMS) supports installation into environments that can provide fail-over or redundancy for both the Cisco TMS server and Cisco TMS database. This document describes the requirements, configuration, and limitations when implementing Cisco TMS in a redundant or fail-over solution. At the time of publication, this document reflects capabilities and requirements as of Cisco TMS version 11.7. Older versions of Cisco TMS prior to 11.5 will differ from this information. Newer versions of Cisco TMS are compatible with these requirements and the document will be revised as necessary to match newer releases of Cisco TMS. Unless stated otherwise, information in this document should apply to all versions of Cisco TMS v11.5 or newer.

The target audience for this document is the Cisco TMS server administrator who wishes to deploy redundancy or fail-over in their Cisco TMS installation. This document assumes the reader has an understanding of Cisco TMS, Cisco TMS installation, Microsoft Windows server operating systems, and an advanced level of understanding of network protocols and networking.

This document is divided into the following sections:

- Overview of Cisco TMS Structures and Communications
- Redundancy Concepts for Cisco TMS
- Cisco TMS Architecture Requirements for Redundancy
- Redundancy Models
- Customer Specific Cisco TMS Files
- Backup and Recovery of the Cisco TMS Database
- Cisco TMS Redundancy Limitations and Notes

Overview of Cisco TMS Structures and Communications

Cisco TMS Server Architecture

Cisco TMS functionality is achieved through the combination of several elements. Users only interact with Cisco TMS through the website, but the complete Cisco TMS product is actually constructed from three different logical components:

Cisco TMS Web-Server: The web server used by Cisco TMS is Microsoft's Internet Information Server (IIS). This provides an interactive interface for users and external systems to interact with Cisco TMS.

Cisco TMS Windows Services: Cisco TMS has a set of Windows services running on the server in the background that handles all background tasks, call set-up, monitoring and application logic. These services are not directly interfaced by users of Cisco TMS.

Cisco TMS Database: The database engine used by Cisco TMS is a Microsoft SQL Server. The database stores most information used by Cisco TMS and is designed to be used simultaneously by multiple agents. The Cisco TMS Website and Cisco TMS Windows Services interact directly with the Cisco TMS database. The database may run on the same server as the rest of Cisco TMS or on a separate server. For most redundancy scenarios the database must run on a separate server.

The Cisco TMS Web server and Cisco TMS Windows Services are installed together on a server when installing Cisco TMS and cannot be installed separately by the installer. The Cisco TMS installation software allows the administrator to selectively choose to install the Cisco TMS database and SQL server locally, or point to an existing remote SQL server.

Communication with Cisco TMS

Users Communicating with Cisco TMS

Users only interface directly to the Cisco TMS website. Best practices dictate that users should access Cisco TMS via a simple DNS name.

Cisco TMS and Devices

Cisco TMS's Windows services and website communicate directly to managed devices through a variety of protocols (HTTP, Telnet, FTP, etc) depending on the device type. In addition, for event reporting and accessing services from Cisco TMS managed devices themselves will initiate connections to Cisco TMS on their own. As such, managed devices are configured with an IP address or DNS hostname on where to access Cisco TMS. This requires the managed devices always have the specific IP address or hostname where Cisco TMS will be reachable.

IP Addresses vs. DNS hostnames

Starting with Cisco TMS v11.5, Cisco TMS specifically is told it's

- local IP address (including IPv6 if IPv6 is configured)
- what local DNS hostname is used to reach the server
- a public DNS hostname used to reach the server

Systems directly reachable by Cisco TMS may configured to use the local Cisco TMS server IP address or local DNS hostname but Cisco TMS will automatically configure device types it knows to support DNS hostnames to use the DNS hostname over IP addresses. For systems that are defined to be 'behind firewall' or 'reachable on public internet' the Cisco TMS Server DNS Hostname (Public) is **required** and used for those systems. Cisco TMS must explicitly be told which value to use for each of these settings.

Cisco TMS and External Systems

External systems such as Exchange Integration or IM integrations always communicate to Cisco TMS through the HTTP protocol. As such, the installation of these packages must always have the specific IP address or DNS hostname where Cisco TMS will be reachable. Using the Cisco TMS Server DNS Hostname (local) value is recommended when using External Integrations with Cisco TMS as it allows for easier to redirect requests to another Cisco TMS server in the case of fail-over.

Cisco TMS and Database

Cisco TMS's Windows services and website communicate to the database very frequently and intensively. While the SQL connection is over IP and could be made over a Wide Area Network, the impact of increased latency would be quite severe on Cisco TMS due to the amount of transactions and the resulting negative impact it would have on the responsiveness of the user interface. As such, the Cisco TMS website and Cisco TMS Services should always be on the same local network as the Cisco TMS database.

Redundancy Concepts for Cisco TMS

Redundancy for your Cisco TMS application can be achieved in several different ways depending on your requirements for availability.

- How long can you tolerate the application being unavailable? - Minutes? Hours? Days?
- Tolerance for data loss – How much data can you lose without causing a significant impact? How much data can you afford to lose in a recovery or fail-over? None? A few minutes? A few hours? A day?
- Administrative capabilities – What resources and skill sets does your organization have internally to administer and configure network and server systems
- Budget/Cost – How much is the organization willing to invest to in networking and server resources to achieve higher availability or fault tolerance for the Cisco TMS application

In general, the higher your demands for accessibility and fault tolerance, the higher the cost and complexity of the redundancy solution. Each solution has pros and cons and administrators must choose which model best suits their business needs.

The redundancy models that can be used with Cisco TMS are:

- Single Server, Single Database, Redundant Hardware
- Single Server, Separate Database
- Single Server, Clustered Database
- Multiple Servers, Manual Cutover
- Multiple Cisco TMS Servers, Load Balancing, and Clustered Database
- Manual Off-Site Fail-over

This document will explain the details of each of these scenarios and in addition outline the requirements of Cisco TMS for any redundancy solution.

Cisco TMS Architecture Requirements for Redundancy

Implementation of Cisco TMS in any redundant or fail-over model hinges on maintaining compatibility with several key concepts from Cisco TMS. The following hold true regardless of which redundancy model you choose to implement. Keeping these concepts in mind will allow you to consider alternative redundancy models or combinations of the ones presented in this document. The requirements are as follows:

- Only one live database per Cisco TMS 'installation'.
  The core of Cisco TMS is its database. You may only have one running copy of the database active at any time. Multiple copies of the database may exist, but only one copy may be 'live' and used at a time Any redundancy methods used for the database will consist of fail-over or backup methods for one database. Two Cisco TMS servers pointing at two different live Cisco TMS databases would be considered two separate installations, not a redundant installation.
- MSDE SQL Server cannot be used.
  Earlier versions of Cisco TMS shipped with the freely distributable version of SQL Server, MSDE 2000. This version is only intended for small deployments. MSDE 2000 is feature limited and can not be used for larger deployments or any deployment that involves multiple Cisco TMS servers or multiple SQL servers. Any deployment considering a redundant solution should be based on Microsoft SQL Server 2000 or SQL Server 2005.
- Local File paths used on the Cisco TMS Servers must be the same across all Cisco TMS Servers.
  The local file system paths used for Cisco TMS files, such as uploaded software files, should be the same on all Cisco TMS servers
- Multiple Cisco TMS servers must all be members of the same domain.
  When using multiple Cisco TMS servers, all Cisco TMS servers must be a member of the same domain and all Cisco TMS users must be members of that domain, or a domain trusted by the Cisco TMS server's domain. Using workgroups and local user accounts is not supported when using multiple Cisco TMS servers.
- You must maintain a low latency (sub 10ms) between a Cisco TMS server and the database.
  User responsiveness will be severely crippled if there is latency between the Cisco TMS servers and the database they are attached to.
- All servers must be time synchronized.
  All servers making up the redundancy solution must be time synchronized through NTP or the Windows Domain
- Each actual Cisco TMS server must be addressable by the managed devices.
  Because devices communicate unsolicited to Cisco TMS, they must be able to communicate directly TO each Cisco TMS server (each server must have a unique, reachable IP address)
- Cisco TMS must 'know' what specific address is to be used to reach the Cisco TMS servers.
  Within Cisco TMS's configuration the Cisco TMS Server Addresses are used to configure what addressees are used to identify Cisco TMS to devices it is managing.. (Note: there are now IPv4 and IPv6 values, and local and public values). In a redundant solution, these addresses could be a Cisco TMS server, or addresses to the load balancer depending on the solution in place. The Cisco TMS configuration values for it's addresses must always be the current, valid addresses to reach Cisco TMS.
- Cisco TMS relies on multiple protocols, not just HTTP.
  Whatever distribution or load balancing model is used, both HTTP and SNMP are used from managed devices for unsolicited connections so both types must be forwarded by a load balancing solution.
- Cisco TMS is multi-vendor and device methods vary between devices.
  Due to difference in vendors and products, not all devices communicate the same to Cisco TMS. Care must be taken to account for all protocols required between Cisco TMS and the devices to be managed
- When using multiple web servers, all should have the same validation key and methods.
  When using multiple web servers, all Cisco TMS websites should be configured with the same

validation key and method to ensure smooth transition if a user gets redirected between machines.

Changes from previous versions

Cisco TMS version 11.0 and 11.5 included enhancements to Cisco TMS's redundancy capabilities. For readers who were familiar with the previous Cisco TMS version 10.0 capabilities, the new improvements are outlined below.

- Snapshots now stored in database.
  Websnapshots will now be available from any Cisco TMS Server, without having to create a fileshare to share between servers to share the snapshot jpegs
- Fail-over support for ongoing conferences.
  Previously if a Cisco TMS Server failed, any ongoing conferences initiated by that individual Cisco TMS Server would lose real-time monitoring updates in Conference Control Center on other Cisco TMS servers. Now, if a Cisco TMS Server fails, the monitoring features of any ongoing conferences that were initiated by the failed server will fail over to a running Cisco TMS server within 2 minutes.
- DNS Hostname support for Cisco TMS addresses.
  Cisco TMS server addresses now support DNS hostname for system types that support DNS resolution. This eliminates the need to manually update management settings on managed devices if a Cisco TMS server IP changes when doing manual fail-over as required in some deployment scenarios.
- Enforce Now management settings command.
  Administrative Tools in Cisco TMS now includes an 'Enforce Now' for management settings which will initiate an immediate update to all systems in Cisco TMS. This eases configuration updates when doing manual fail-over as required in some deployment scenarios.
- Cisco TMS Service Reporting in Administrative Tools.
  The Administrative Tools page in Cisco TMS now includes status reports of services from all Cisco TMS servers connecting to the Cisco TMS database. This allows an administrator to monitor the health of all Cisco TMS services across multiple servers directly from Cisco TMS.
- Improved database connection resiliency for services.
  The service components of Cisco TMS now include greater resiliency to the database server failing by including the ability to startup with no database online, and then implementing retries to wait for the database server to become available.
- Cisco TMS Pages are now stateless bullet removed as some elements will require consistent web validation keys for pages to operate properly and we will recommend HTTP 'sticky sessions'.

Redundancy Models for Cisco TMS

This section will outline each of the redundancy models covered in this document highlighting their concept, recovery models, advantages, disadvantages, installation, maintenance, and upgrade requirements.

Single Server, Single Database, Redundant Hardware

The first level of any redundant solution should consist of installing Cisco TMS onto a server-grade platform that includes:

- ECC Memory – To protect against memory failure.
- RAID Disks – To protect against hard drive failure.
- Redundant Power Supplies – To protect against power supply failure.

These steps provide the first line of defense against an equipment failure and should be part of any high availability Cisco TMS installation. In this scenario, the Cisco TMS server and SQL server are installed on the same server, so if this server were to be taken offline due to network or equipment failure, Cisco TMS would be unavailable. There is no direct fail-over available, but service can be restored quickly by getting the server back online, or replacing the server with another using the same IP and configuration.

Recovery Methods:

- Repair the existing server and bring it back online
  or
- Replace failed server with new server using same IP address as original Cisco TMS. Install a new copy of Cisco TMS. Restore customer specific Cisco TMS data files (See Section 0 Customer specific TMS Files) and restore the SQL database from backup (See Section 0 Backup and Recovery of the TMS database).

Installation

The Cisco TMS installation program allows selecting where to install the Cisco TMS software on the local disks as part of the custom installation. Cisco TMS should be installed onto the RAID portion of the hard disks. Setup and Maintenance of the redundant features of the server platform are provided by the server vendor.

Maintenance

Users should regularly backup the SQL database. The interval between backups defines the maximum time window over which data would be lost. Typical installations would perform full nightly backups of the database. Please see Backup and Recovery of the TMS database section of this document for additional details on how to perform backups and restores of the Cisco TMS database.

Upgrading Cisco TMS

This installation model requires no additional steps or procedures to the normal upgrade process for Cisco TMS.

Model Summary

- Immediate fail-over available – No
- Amount of data lost – Call data during outage can be lost for some system types. No system or configuration data lost if restored from database backup. Call and Scheduling information created since last backup will be lost if the database is restored from a backup
- Time to restore service – Dependant on time to repair the server or replace with an another server and restore backups (estimate from a few hours to a day)

- Administrative capabilities required – Low, only requires basic skills and SQL backup/recovery procedures
- Cost – Low, cheapest alternative available

Single Server, Separate Database

The first level of any redundant solution should consist of installing Cisco TMS onto a server-grade platform that includes:

- ECC Memory – To protect against memory failure
- RAID Disks – To protect against hard drive failure
- Redundant Power Supplies – To protect against power supply failure

These steps provide the first line of defense against an equipment failure and should be part of any high availability Cisco TMS installation. In addition, you can install the SQL database onto an existing, separate server from Cisco TMS. This is done primarily for performance and manageability from an administrator's perspective. From a performance perspective, putting the SQL database on a separate server reduces the CPU load and significantly reduces the memory load on the Cisco TMS server. Using an existing SQL server offers the management benefit of not having an additional SQL Server to maintain on the network for a single application.

In this scenario, the Cisco TMS server and SQL server are installed on separate servers, but if either server were to be taken offline due to network or equipment failure, Cisco TMS would be unavailable. There is no direct fail-over available, but service can be restored relatively quickly by getting the servers back online, or replacing the servers with another using the same IP and configuration.

Recovery Methods:

- Cisco TMS Server Failure
  - Repair the existing server and bring it back online
    or
  - Replace failed server with new server using same IP address and DNS hostname as the original Cisco TMS. Install a new copy of Cisco TMS from the installation media. During the install, select custom installation and point the installer at the existing SQL database. The install will continue as normal and after installation your Cisco TMS server will be have the configuration used prior to the failure. You should also restore customer specific Cisco TMS data files (See Section 0 Customer specific TMS Files) if the server is replaced.
- SQL Server Failure.
  - Repair the existing server and bring it back online
    or
  - Replace the failed server with a new server and re-install the SQL server. The user account previously used to connect Cisco TMS to the SQL server should be re-created (if a custom one was used) and the password reset to the original password used. Create a new empty database named tmsng and assign database owner privileges on the database to the SQL user created. Once the SQL user and database have been recreated, the database can be restored from a previous backup. Please see Section 0 Backup and Recovery of the TMS database for details on performing a SQL database recovery.

Installation

The separate SQL Server should be installed and operational prior to installing Cisco TMS. You do not need to perform any special operations on the SQL server prior to Cisco TMS installation except 'mixed mode authentication' must be enabled. Using the 'custom' option in the Cisco TMS installer, you can point the installer to the existing SQL server and the installer will handle creating the database on the SQL Server as part of the installation process. The database files will be created per the database defaults of the SQL Server. The Cisco TMS Tools application installed with Cisco TMS should be used to update SQL connection settings post-install if required.

Maintenance

Users should regularly backup the SQL database. The interval between backups defines the maximum time window over which data would be lost. Typical installations would perform full nightly backups of the database. Please see Section 0 Backup and Recovery of the TMS database of this document for additional details on how to perform backups and restores of the Cisco TMS database.

Upgrading Cisco TMS

This installation model requires no additional steps or procedures to follow when performing upgrades or patches.

Model Summary

- Immediate fail-over available – No
- Amount of data lost – Call data during outage can be lost for some system types if Cisco TMS Server is down. No system or configuration data lost if SQL Server does not fail. If SQL Server fails, Cisco TMS is unavailable until the SQL Server is restored to service. Call and Scheduling information created since last backup will be lost if database restored from backup
- Time to restore service – For the Cisco TMS Server, it is dependent on time to repair the server or replace with another server on the same IP address and DNS hostname and perform a recovery. For the SQL Server, it is dependent on time to repair the server or replace with another server on the same IP address and perform a recovery. Estimate a few hours to a day.
- Administrative Capabilities Required – Low, only requires basic skills and SQL backup/recovery procedures
- Cost – Low, only requires a second server which may be tasked with other SQL jobs

Single Server, Clustered Database

This model is identical to the previous Section 0 Single Server, Separate Database

except the remote SQL Server is a part of a SQL Server cluster, rather than a stand-alone server. SQL Clustering allows multiple servers to operate as a group and provide fail-over for a SQL Server in case of a failure. A SQL cluster consists of a shared disk array that can be accessed by multiple nodes. Virtual SQL Servers are created and hosted on a node, with the information for each Virtual Server being stored on the shared disk array. When a node fails, any Virtual Server being hosted by the node can automatically fail-over to another node in the cluster and continue operation. The SQL Cluster itself and the fail-over of the SQL Server is transparent to Cisco TMS as the Cluster serves the database via a virtual IP address or name. For more information on SQL Clustering requirements, capabilities, and configuration, please see Microsoft's SQL Server 2000 documentation.

http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/failclus.mspx

http://www.microsoft.com/sql/techinfo/administration/2000/availability.mspx

One of the main benefits of using a SQL cluster is you can pool redundancy resources to share among several servers. An organization may already have a high performance, high availability SQL Cluster. Using this cluster will provide Cisco TMS redundancy with quick fail-over to prevent failure of the database component of Cisco TMS.

In this scenario, if the Cisco TMS server were taken offline due to network or equipment failure, Cisco TMS would be unavailable. If the SQL Server were to fail, the SQL cluster would detect the server becoming unavailable and would initiate a fail-over to another server in the cluster. The time required to fail-over is specific to your SQL Cluster configuration, but normally is on the order of seconds to minutes and can be fully automatic, with no administrative input.

Recovery Methods

- Cisco TMS Server Failure
  - Repair the existing server and bring it back online or
  - Replace failed server with new server using same IP address and DNS hostname as the original Cisco TMS. Install a new copy of Cisco TMS from the installation media. During the

install, select custom installation and point the installer at the existing SQL database. The install will continue as normal and after installation your Cisco TMS server will be have the configuration used prior to the failure. You should also restore customer specific Cisco TMS data files (See Section 0 Customer specific TMS Files) if the server is replaced.

- SQL Server Failure – The SQL Cluster will automatically handle the fail-over of assigning the SQL Server resources to another node in the cluster. This happens transparently to Cisco TMS. Please refer to the Microsoft SQL Server documentation for information on restoring a node in a SQL Cluster.

Installation

Configuring a Microsoft SQL Cluster is outside the scope of this document. Please refer to Microsoft's documentation for additional details

http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/failclus.mspx

Prior to installing Cisco TMS, the SQL Cluster should be active and must have the Virtual SQL Server installed and active that you wish to use for Cisco TMS. The Virtual SQL Server will have an instance name and IP Address to reach the SQL server.

Once the Virtual SQL Server is configured, Cisco TMS can be installed on the separate Cisco TMS server. The Cisco TMS installation program allows you to select an existing remote SQL server as part of the custom installation. Select or enter the instance name or IP address of the Virtual SQL Server. The installation program will fully handle the configuration of the database on the existing SQL server. The database files will be created on the Virtual SQL Server per the database defaults of the SQL Server. The Cisco TMS Tools application installed with Cisco TMS should be used to update SQL connection settings post-install if required.

Maintenance

Users should regularly backup the SQL database. The interval between backups defines the maximum time window over which data would be lost. Typical installations would perform full nightly backups of the database. Please see Section 0 Backup and Recovery of the TMS database of this document for additional details on how to perform backups and restores of the Cisco TMS database.

Upgrading Cisco TMS

This installation model requires no additional steps or procedures to follow when performing upgrades or patches.

Model Summary

- Immediate fail-over available.
  Yes for SQL Server. No for Cisco TMS Server
- Amount of data lost.
  Call data during outage can be lost for some system types if Cisco TMS Server is down. If SQL Server fails, SQL Cluster will fail-over and Cisco TMS will still be available. No data is lost when the SQL Server fails over
- Time to restore service.
  For SQL Server, recovery is dependent on SQL Server configuration, normally on the order of seconds to minutes. For the Cisco TMS Server, it is dependent on time to repair the server or replace with another server on the same IP address and DNS hostname and perform a recovery. Estimate a few hours to a day.
- Administrative Capabilities Required.
  Low for Cisco TMS Server portion, very high for SQL Cluster.
- Cost.
  High if the SQL Cluster does not already exist

Multiple Servers, Manual Cutover

While the previous sections have covered redundancy for the SQL database, they do not provide solutions for quick fail-over for the Cisco TMS Server itself which hosts the Cisco TMS website and the Cisco TMS Windows Services. To speed recovery time for the Cisco TMS server, you can install additional 'warm spares' of the Cisco TMS server. In this model, there are multiple Cisco TMS servers, all pointed to the same separate SQL server, but only one Cisco TMS Server is considered the active server. The secondary machines are configured, but are disabled to remain inactive. Then, if the primary Cisco TMS server fails, a secondary Cisco TMS server can quickly be activated, allowing Cisco TMS to be available while the primary server is being worked on. The SQL database can be redundant as well if deployed using a SQL Server Cluster.

In this scenario you have multiple servers on different addresses and but only one Cisco TMS server can actively receive events and activity from users. Theoretically while individual devices and users could be directed to different Cisco TMS servers, this will lead to erroneous warnings in Cisco TMS for device configurations. In addition, the Cisco TMS Services installed on the secondary machines will be active and actually process events and call activity.

Note: To prevent confusion and assist in troubleshooting, Cisco TelePresence recommends you **not** run the Cisco TMS services on the secondary servers while they are not the active Cisco TMS server.

This model can be thought of as a 'manual' fail-over between multiple Cisco TMS servers to reduce downtime, but at the added cost of having additional stand-by servers.

Error! Objects cannot be created from editing field codes.

Figure 1 Multiple Stand-by Server Illustration

Recovery Methods

- Cisco TMS Server Failure.
  - Repair the existing server and bring it back online or,
  - Free up the IP address normally used by Cisco TMS by changing the primary server's IP address to an alternative IP address. Reconfigure one of the secondary Cisco TMS servers to be the IP Address and DNS hostname of the primary Cisco TMS server which is no longer online. Activate the Cisco TMS Services (all services whose names start with Cisco TMS and the WWWPublishingService). This machine is now the primary Cisco TMS server. Alternatively: If managing only systems that support DNS hostnames for management settings, you can simply update the DNS hostname record to point to the new server's IP address, update the Cisco TMS Server Local IPv4 Address (and IPv6 if in use) configuration value and start all services on the new Cisco TMS server.
- SQL Server Failure – The SQL Cluster will automatically handle the fail-over of assigning the Virtual SQL Server resources to another node in the cluster. This happens transparently to Cisco TMS. Please refer to the Microsoft SQL Server documentation for information on restoring a node in a SQL Cluster.

Installation

Using multiple Cisco TMS Servers requires the use of a separate SQL server, either stand-alone or clustered.

Stand-alone SQL Server

The separate SQL Server should be installed and operational prior to installing Cisco TMS. You do not need to perform any special operations on the SQL server prior to Cisco TMS installation except 'mixed mode authentication' must be enabled.

Clustered SQL Server

Configuring a Microsoft SQL Cluster is outside the scope of this document. Please refer to Microsoft's documentation for additional details

http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/failclus.mspx

Prior to installing Cisco TMS, the SQL Cluster should be active and must have the Virtual SQL Server installed and active that you wish to use for Cisco TMS. The Virtual SQL Server will have an instance name and IP Address to reach the SQL server and 'mixed mode authentication' must be enabled.

Installing the Cisco TMS servers

Domain Requirements.

Since you will be using multiple Cisco TMS servers, all Cisco TMS servers must be a member of a domain, and all Cisco TMS users should be a member of that domain or a domain trusted by the Cisco TMS server's domain. Using Windows local user accounts is not supported when using multiple Cisco TMS servers.

Installing primary TMS application.

Once the SQL Server is configured, begin by installing Cisco TMS on what is to be the primary Cisco TMS server. By choosing custom during installation, the program allows you to select the existing remote SQL server as part of the installation. Select or enter the instance name or IP address of the SQL Server (Virtual SQL Server if using clustering). The installation program will fully handle the configuration of the database on the existing SQL server. The database files will be created per the database defaults of the SQL Server. The Cisco TMS Tools application installed with Cisco TMS should be used to update SQL connection settings post-install if required.

Installing secondary TMS application.

Once the primary server is installed, you may install additional Cisco TMS servers to be your inactive 'warm standby' servers. Each of the warm stand-by servers will be a separate server, with its own IP address and machine name. Perform the installation on the secondary servers following the same steps as used on the primary Cisco TMS server. Each Cisco TMS install must be consistent with the other servers, so you must use the same local file paths on each server installation (Example: Cisco TMS installation path and Software Directory). After the Cisco TMS installation completes, you will be prompted to reboot the server. Reboot the server. After the server restarts, you must make the Cisco TMS portion of the server inactive by stopping all the Cisco TMS and Web services and setting them to manual startup. Open the Services tool from Administrative Tools in the Windows smart menu, and stop all services whose name starts with Cisco TMS and the WWWPublishingService service. Right-click on each of these services and select Properties. On the General tab of each of the services you stopped, set startup type to Manual. The server now has Cisco TMS installed, but is not actively running. Repeat these steps for each additional 'warm spare' server you wish to have. When promoting a server to be the primary Cisco TMS server, you should change these services back to Automatic so they restart on server power-up. Only the active primary Cisco TMS server should have it's services set to Automatic.

Custom file synchronization.

Part of the Cisco TMS installation will consist of files added or customized by users and administrators. These files must be synchronized to all Cisco TMS servers being used. The setup of this synchronization should be configured as part of the installation process. Please see Section 0 Customer specific TMS Files for more details on these files and methods to synchronize them between servers.

Set primary TMS address

After all the warm spares have been installed, log into the primary Cisco TMS server's website, go to Administrative Tools>Configuration>Network and change the Cisco TMS Server IPv4 Address (Local):

address to the IP address of the primary Cisco TMS server. This is the IP address Cisco TMS will use for enforce management settings and to compare for device configuration errors. This setting is stored in the Cisco TMS database, and therefore will be shared among all servers. This value will be overwritten anytime you run the Cisco TMS installer on a server connected to the database so it must be verified to be the primary Cisco TMS server's IP after running any Cisco TMS installation software. The Cisco TMS Server DNS hostname values should also be configured to point to the primary Cisco TMS server, but these will not be overwritten by upgrades or additional installs.

After Cisco TMS is installed, you should configure a DNS hostname record to point to the IP address of the primary Cisco TMS server. Cisco TelePresence recommends you use the DNS hostname over IP addresses for user access to Cisco TMS, configuring external integrations with Cisco TMS (such as Exchange or Lotus) and is required when using the Remote/SOHO support or public/local identity features of Cisco TMS.

Set web validation key on web servers

When running multiple web servers, each web server must use the same encryption method for the viewstate information of the pages. This is achieved by specifying the machine key to be used by IIS rather then letting IIS generate its own which is the default behavior. The machinekey behavior can be controlled using the web.config file used by the Cisco TMS web application. This file is located in the wwwCisco TMS directory (default c:\program files\tandberg\tms\wwwCisco TMS) The behavior of this element is described in the following Microsoft articles

http://msdn2.microsoft.com/en-us/library/w8h3skw9(VS.71).aspx

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpag2/html/paght000007.asp

Microsoft provides sample code to generate these keys, but there are several public websites that simplify the creation of these keys for you. Some example sites are

http://www.orcsweb.com/articles/aspnetmachinekey.aspx

http://www.aspnetresources.com/tools/keycreator.aspx

Example machinekey string:

```
<configuration>
    <system.web>
        <machineKey
validationKey='50C6CA92F369A87AB487E3678C7D229119A47F921C8266D9FB0DE2B28829
CDECDD5FEEE7CC534497A90D0AB3B8FB9F81021A7DC00ACC6F39D67EA9036C1F8733'
decryptionKey='52480E9648080C4A87BB434CF281064243E3C09B003C49D0'
validation='SHA1'/>
    </system.web>
</configuration>
```

Create a machinekey element using Microsoft's supplied methods or from the sample websites listed above. Open the web.config file under the wwwCisco TMS directory and insert the new machinekey element text under the existing <system.web> element in the document. You must update the web.config file on each of the Cisco TMS servers. Be sure to use the same machinekey string on all servers.

Maintenance

Users should regularly backup the SQL database. The interval between backups defines the maximum time window over which data would be lost. Typical installations would perform full nightly backups of the database. Please see Section 0 Backup and Recovery of the TMS database of this document for additional details on how to perform backups and restores of the Cisco TMS database.

As multiple Cisco TMS servers are being used, administrators should periodically check that their file synchronization process is still functioning to ensure smooth cut-over in the case of having to use a warm spare.

Upgrading TMS

All Cisco TMS servers accessing the same database must be running the same Cisco TMS version. When upgrading between Cisco TMS versions, there will be inconsistencies between different servers as each is upgraded so extra steps are required when performing Cisco TMS upgrades or patches.

When performing a Cisco TMS upgrade, the following steps must be followed

- Plan an upgrade during a time window when Cisco TMS can be made unavailable to users as Cisco TMS will be unavailable during the duration of your upgrade.
- On your primary Cisco TMS server, start the installer for the Cisco TMS upgrade as normal. During this process, any updates to the SQL database will be performed.
- Installation may require a reboot of the server. After the reboot, go into Services component of Computer Management on the server, manually stop all services whose name starts with Cisco TMS and the WWWPublishingService service.
- Proceed to the next server, and start the installer for the Cisco TMS upgrade the same as you did on the primary Cisco TMS server.
- The installer will likely restart the Cisco TMS services and WWWPublishingService and may require a reboot of the server. After the reboot, go into Services component of Computer Management on the server, manually stop all services whose name starts with Cisco TMS and the WWWPublishingSevice. The services may also be configured for automatic startup. Right-click on each of these services and select Properties. On the General tab of each of the services you stopped, set startup type to Manual.
- After upgrading all Cisco TMS servers, log into the primary Cisco TMS's Windows console and restart all Cisco TMS services and WWWPublishingService. Secondary servers should all still have their Cisco TMS and WWWPublishingService stopped and set to manual startup.
- Log into the Cisco TMS website, go to **Administrative Tools>Configuration>Network** and change the Cisco TMS Server IPv4 Address (Local): address to the IP address of the primary Cisco TMS server. Your upgrade is now complete.
- Upgrades will erase any changes to the IIS web configuration files, including the viewstate machine key and method defined during installation. Repeat the viewstate key generation and installation steps outlined in the Installation section on each of the upgraded web servers.

Model Summary

- Immediate fail-over available.
  Yes for SQL Server. No for Cisco TMS Server
- Amount of data lost.
  Call data during outage can be lost for some system types if Cisco TMS Server is down. If SQL Server fails, SQL Cluster will fail-over and Cisco TMS will still be available. No data is lost when the SQL Server fails over. Please be sure to read Section 0 Cisco TMS Redundancy limitations and notes for specific notes about processes during a server failure.
- Time to restore service.
  For clustered SQL servers, depending on configuration, normally on the order of seconds to minutes. For a stand-alone SQL Server, it is dependant on time to repair the server or replace with another server on the same IP address and perform a recovery. Estimate a few hours to a day. For the Cisco TMS Server, it is dependant on time to repair the server or activate the 'warm standby'. Activating the warm stand-by can be done in just a few minutes.
- Administrative Capabilities Required.
  Low for Cisco TMS Server portion and stand-alone SQL server, very high if SQL Cluster must be created
- Cost.
  Medium as you must now have a minimum of three servers

Multiple TMS Servers, Load Balancing, and Clustered Database

The highest availability configuration is one that will provide automatic fail-over for both the Cisco TMS Server and the SQL database. Automatic Fail-over for the SQL database is discussed in Section 0 Single Server, Clustered Database. Combining a SQL Cluster with multiple Cisco TMS Servers being fronted by a Network Load Balancer (NLB) will provide fully automatic fail-over for both Cisco TMS and the SQL Server.

Managed devices must be configured with the IP address or DNS hostname of the Cisco TMS server so those addresses must be 'shared' between all the Cisco TMS Servers. Simply pointing a unit to multiple management servers is not sufficient as the management servers must be performing in unison to not duplicate tasks and to share information properly. The Network Load Balancer performs this 'sharing' function by forwarding connections sent to these 'shared' addresses to a particular Cisco TMS server from a pool of Cisco TMS servers. Depending on the particular NLB being used, the logic behind which Cisco TMS server the connection gets forwarded to can be customized. The NLB must be able to forward all HTTP connections and SNMP Traps sent to the 'shared' addresses. Due to view state in web functionality, sticky connections should be enabled in the load balancer to ensure the same web session stays on the same web server.

Error! Objects cannot be created from editing field codes.

Figure 2 Network Load Balancing

When the Cisco TMS servers need to initiate connections to managed devices, each server can initiate the connection directly from the server to the managed device. Therefore it is required that the individual Cisco TMS servers be directly addressable by their own IP address from the managed systems, not just through the NLB.

In this deployment scenario, fail-over for Cisco TMS servers is handled by the forwarding logic of the NLB. The NLB should know not to forward connections to a Cisco TMS server that is not responding. Fail-over for the Cisco TMS database is handled automatically by the SQL Cluster.

Recovery Methods

- Cisco TMS Server Failure.
  The NLB should not forward connections to a failed Cisco TMS server, so fail-over to another Cisco TMS server is automatic. The Failed server should be repaired and brought back online when possible.
- SQL Server Failure.
  The SQL Cluster will automatically handle the fail-over of assigning the SQL Server resources to another node in the cluster. This happens transparently to Cisco TMS. Please refer to the Microsoft SQL Server documentation for information on restoring a node in a SQL Cluster

Installation

- Domain Requirements.
  Since you will be using multiple Cisco TMS servers, all Cisco TMS servers must be a member of a domain, and all Cisco TMS users should be a member of that domain or a domain trusted by the Cisco TMS server's domain. Using Windows local user accounts is not supported when using multiple Cisco TMS servers.
- Setup SQL Cluster.
  The SQL Cluster must be configured before installing Cisco TMS. Configuring a Microsoft SQL Cluster is outside the scope of this document. Please refer to Microsoft's documentation for additional details

http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/failclus.mspx

Prior to installing Cisco TMS, the SQL Cluster should be active and must have the Virtual SQL Server installed and active that you wish to use for Cisco TMS. The Virtual SQL Server will have an instance name and IP Address to reach the SQL server and 'mixed mode authentication' must be enabled.

- Installing primary Cisco TMS application.
  Once the Virtual SQL Server is configured, Cisco TMS can be installed on the first Cisco TMS server. The Cisco TMS installation program allows you to select an existing remote SQL server as part of the custom installation. Select or enter the instance name or IP address of the Virtual SQL Server. The installation program will fully handle the configuration of the database on the existing

SQL server. The database files will be created on the Virtual SQL Server per the database defaults of the SQL Server. The Cisco TMS Tools application installed with Cisco TMS should be used to update SQL connection settings post-install if required.

- Installing secondary Cisco TMS application.
  Once the primary server is installed, you may install additional Cisco TMS servers to use behind the load balancer. Each of the servers will be separate servers, with their own IP address and machine name. Perform the installation on the additional servers following the same steps as used on the primary Cisco TMS server. Each Cisco TMS install must be consistent with the other servers, so you must use the same local file paths on each server installation (Example: Cisco TMS installation path and Software Directory). After the Cisco TMS installation completes, you will be prompted to reboot the server. Reboot the server. Repeat these steps for each additional server you wish to have being fronted by the load balancer.
- Custom file synchronization.
  Part of the Cisco TMS installation will consist of files added or customized by users and administrators. These files must be synchronized to all Cisco TMS servers being used. The setup of this synchronization should be configured as part of the installation process. Please see Section 0 Customer specific TMS Files for more details on these files and methods to synchronize them between servers.
- Set primary Cisco TMS address.
  After all the Cisco TMS servers have been installed, log into the website of one of the Cisco TMS servers, go to **Administrative Tools> Configuration >Network** and change the Cisco TMS Server Addresses (all 4 as required) addresses that will be forwarded by the network load balancer. These are the addresses Cisco TMS will provide to managed devices to contact Cisco TMS and to compare for device configuration errors. These settings are stored in the Cisco TMS database, and therefore will be shared among all servers. The Cisco TMS Server IPv4 Address (Local) and Cisco TMS Server IPv6 Address (Local) values will be overwritten anytime you install a Cisco TMS server against the Cisco TMS database so these values must be verified to be the addresses forwarded by the NLB after any Cisco TMS install or upgrade is ran.
- Set web validation key on web servers
  When running multiple web servers, each web server must use the same encryption method for the viewstate information of the pages. This is achieved by specifying the machine key to be used by IIS rather then letting IIS generate its own which is the default behavior. The machinekey behavior can be controlled using the web.config file used by the Cisco TMS web application. This file is located in the wwwCisco TMS directory (default c:\program files\tandberg\tms\wwwCisco TMS) The behavior of this element is described in the following Microsoft articles

http://msdn2.microsoft.com/en-us/library/w8h3skw9(VS.71).aspx
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpag2/html/paght000007.asp

Microsoft provides sample code to generate these keys, but there are several public websites that simplify the creation of these keys for you. Some example sites are

http://www.orcsweb.com/articles/aspnetmachinekey.aspx
http://www.aspnetresources.com/tools/keycreator.aspx

Example machinekey string:

```
<configuration>
    <system.web>
        <machineKey
validationKey='50C6CA92F369A87AB487E3678C7D229119A47F921C8266D9FB0DE2B28829
CDECDD5FEEE7CC534497A90D0AB3B8FB9F81021A7DC00ACC6F39D67EA9036C1F8733'
decryptionKey='52480E9648080C4A87BB434CF281064243E3C09B003C49D0'
validation='SHA1'/>
    </system.web>
</configuration>
```

Create a machinekey element using Microsoft's supplied methods or from the sample websites listed above. Open the web.config file under the wwwCisco TMS directory and insert the new machinekey element text under the existing <system.web> element in the document. You must update the web.config file on each of the Cisco TMS servers. Be sure to use the same machinekey string on all servers.

- Setup Network Load Balancer.
  Next, the Network Load Balancer should be installed and configured. Specific instructions will vary based on the NLB type used, but the following requirements must be met for use with Cisco TMS. Devices must be able to access a specific IP Address and DNS hostname that will be forwarded by the NLB
  - The NLB must only forward a connection to a single server, not multiples
  - The NLB must be able forward HTTP and SNMP Trap traffic
  - The NLB should use sticky connections for web sessions for the best results
  - The NLB must maintain its own rules for determining which servers are available and which to forward to:
    The IP address and DNS hostname being forwarded by the NLB must be configured in Cisco TMS as the as the Cisco TMS Server Addresses because Cisco TMS must know which address to provide managed devices to reach Cisco TMS. . The appropriate address (local or public) should be the entered in all managed devices and external integrations as the management address or address to reach Cisco TMS. Please reference the Cisco TMS Device Support Document available on the Cisco TMS installation media for configuration details for each managed device type. Once the NLB is configured and operational, you may continue to configure Cisco TMS as normal through its web interface and add devices and other external integrations.

Maintenance

Users should regularly backup the SQL database. The interval between backups defines the maximum time window over which data would be lost. Typical installations would perform full nightly backups of the database. Please see the Section 0 Backup and Recovery of the TMS database of this document detailing backup and restore procedures for SQL server.

As multiple Cisco TMS servers are being used, administrators should periodically check that their file synchronization process is still functioning to ensure seamless use of any Cisco TMS server.

Upgrading TMS

All Cisco TMS servers accessing the same database must be running the same Cisco TMS version. When upgrading between Cisco TMS versions, there will be inconsistencies between different servers as each is upgraded so extra steps are required when performing Cisco TMS upgrades or patches.

When performing a Cisco TMS upgrade, the following steps must be followed

- Plan an upgrade during a time window when Cisco TMS can be made unavailable to users as Cisco TMS will be unavailable during the duration of your upgrade
- Log into the Windows console of each Cisco TMS server, and from the Services component of Computer Management, manually stop all services whose name starts Cisco TMS and the WWWPublishingSevice service. Repeat this step on all Cisco TMS servers that are part of the pool. All Cisco TMS services and websites should be stopped on all servers before proceeding.
- Start on a single Cisco TMS server. Start the installer for the Cisco TMS upgrade as normal. During this process, any updates to the SQL database will be performed.
- The installer will likely restart the Cisco TMS services and WWWPublishingService and may require a reboot of the server. After the reboot, go into Services component of Computer Management, manually stop all services whose name starts with Cisco TMS and the WWWPublishingSevice
- Proceed to the next server, and start the upgrade or patch installer the same as you did on the first Cisco TMS server. Make sure to manually stop the Cisco TMS services and website after the

installation completes and the server reboots if necessary. Repeat these steps one server at a time until all Cisco TMS servers have been upgraded

- Once all Cisco TMS servers have been upgraded, you may restart all Cisco TMS services and WWWPublishingService on all Cisco TMS servers.
- Log into the Cisco TMS website, go to **Administrative Tools>Configuration>Network** and change the Cisco TMS Server IPv4 Address (Local): address to the IP address that is forwarded by the network load balancer. Your upgrade is complete
- Upgrades will erase any changes to the IIS web configuration files, including the viewstate machine key and method defined during installation. Repeat the viewstate key generation and installation steps outlined in the Installation section on each of the upgraded web servers

Model Summary

- Immediate fail-over available.
  Yes for SQL Server. Yes for Cisco TMS Server
- Amount of data lost.
  No data will be lost if fail-over has occurred, as Cisco TMS and the SQL Server can failover automatically. Please be sure to read Section 0 Cisco TMS Redundancy limitations and notes for specific notes about processes during a server failure.
- Time to restore service.
  For SQL Server, recovery is dependant on SQL Server configuration, normally on the order of seconds to minutes. For Cisco TMS Server, dependant on NLB configuration but should be transparent to the users
- Administrative Capabilities Required.
  High for Network Load Balancer and handling multiple Cisco TMS servers. Very high for SQL Cluster.
- Cost.
  Highest. Must implement multiple servers, Network Load Balancer, and SQL Cluster if it does not already exist

Manual Off-Site Fail-Over

While using a network load balancer and SQL cluster will provide automatic fail-over for both the Cisco TMS server and SQL database, the solution requires all the servers be located together. Some customers require a fail-over solution that allows cut-over to an installation off-site from the primary installation in case of catastrophic network failure at the primary site. The basis of an off-site fail-over is to maintain a copy of the Cisco TMS Server and Cisco TMS database that are inactive in an off-site location. When fail-over is required, an administrator cuts over to the secondary location. One solution for this is to use Log Shipping, a functionality of Microsoft SQL Server to keep the database in the secondary location up to date. Log Shipping allows you to have one main database, and a separate fail-over database. Log Shipping allows all changes to the main database to be batch transferred to the fail-over database off-site. This model uses a complete 'copy' of the primary system off-site, so this technology can be combined with other redundancy models within each location if desired. It is critical that when combining this model with other methods, such as using a Network Load Balancer at each location, that the off-site location must be completely disabled; all Cisco TMS services and websites, until the off-site location is activated to become the primary site.

Microsoft references on SQL Server Log Shipping

http://www.microsoft.com/technet/prodtechnol/sql/2000/deploy/hasog02.mspx

Log shipping to a secondary site provides high resiliency to network failure, but has some disadvantages as well.

Error! Objects cannot be created from editing field codes.

Figure 3 Balancing Off-Site Cutover

- The secondary SQL server is not always a current version of the database, as updates are 'batched' job transferred to the secondary server. Shipping intervals are defined in the SQL Server
- The bandwidth and processing required to ship updates to the back-up server limits how frequently you can update the back-up server
- The secondary Cisco TMS server must be kept offline and disabled until the off-site is brought online to be the primary site.
- Fail-over to the secondary site requires changing the address users and devices use to reach Cisco TMS. For users, a DNS name could be updated, but may take time to propagate. Managed Device management settings can be updated in bulk from Cisco TMS's Administrative Tools.
- Cutting back to the primary site can be complicated as the database must be re-synchronized from what has been changed in the secondary SQL server

Recovery Methods

- Primary Site Failure.
  The primary server must completely disabled before the secondary Cisco TMS server can be activated. The primary site's SQL server should be disabled to ensure it does not start up unexpectedly. The secondary Cisco TMS server must be started by activating all services whose name starts with Cisco TMS and the WWWPublishingService service. Log into the website of the secondary Cisco TMS server and update the Cisco TMS Server IPv4 Addresses (and IPv6 if in use) under **Administrative Tools>Configuration>Network** to the IP address of the secondary Cisco TMS server. The DNS hostname used to point to Cisco TMS should be updated to match the IP address of the secondary Cisco TMS server. The management addresses of all managed devices must be updated to match these new settings. The Enforce Now button on the Network page under **Administrative Tools>Configuration** can automate this process for managed devices. Please refer to the Cisco TMS Product Support document available on the Cisco TMS Installation Media for information on what settings must be configured per device type. Any external integrations must have their Cisco TMS address updated to point to the secondary Cisco TMS Server's address as well if the DNS hostname was changed or if they used an IP address instead of hostname. After these changes, all activity will be directed to the secondary site. Recovery to the primary site is done in the same fashion except in addition the primary site's SQL server must be updated from the secondary SQL Server. Please see Microsoft's documentation on Log Shipping for details on how to recovery the primary SQL server before activating the primary site's Cisco TMS server.

Note: If you use daily configuration restore, you should create new backups of systems after updating the management settings of systems to prevent the restore from setting the old values back onto the systems. If you use any persistent templates that include management settings, these too should be updated to the new Cisco TMS server address.

Installation

Configuring Microsoft SQL Log Shipping is outside the scope of this document. Please refer to Microsoft's documentation for additional details

http://www.microsoft.com/technet/prodtechnol/sql/2000/deploy/hasog02.mspx

The database Cisco TMS will create and use is named tmsng. This is the database that must be replicated to the secondary SQL server.

Cisco TMS and the SQL Server in the primary site should be installed and configured per the model you have chosen. Once Cisco TMS is configured, Log Shipping to the secondary SQL Server site can be configured per Microsoft's directions. Once the secondary SQL Server is configured and has the tmsng database being published from the primary SQL server, you can install Cisco TMS in the secondary site. Simply install Cisco TMS according to the deployment model you are using and point the installation to the secondary site's SQL Server. Each Cisco TMS install must be consistent with the other servers, so you must use the same local file paths on each server installation (Example: Cisco TMS installation path and Software Directory).

After the Cisco TMS installation completes, you will be prompted to reboot the server. Reboot the server. After the server restarts, you must make the Cisco TMS portion of the server inactive by stopping all the Cisco TMS and Web services and setting them to manual startup. Open the Services tool from Administrative Tools in the Windows smart menu, and stop all services whose name starts with Cisco TMS and the WWWPublishingService service. Right-click on each of these services and select Properties. On the General tab of each of the services you stopped, set startup type to Manual. The server now has Cisco TMS installed, but is not actively running. Repeat these steps for each additional 'warm spare' server you wish to have.

Part of the Cisco TMS installation will consist of files added or customized by users and administrators. These files must be synchronized from the primary server to the off-site server. The setup of this synchronization should be configured as part of the installation process. Please see Section 0 Customer specific TMS Files for more details on these files and methods to synchronize them between servers.

After the off-site Cisco TMS server has been installed, and the customer specific files have been setup to be copied, no further configuration is required. The SQL database at the off-site location will be updated from the primary site, and therefore no Cisco TMS configuration is required on the off-site Cisco TMS server. The off-site Cisco TMS server should always be off-line unless it is being upgraded or is being promoted to the active server.

Maintenance

Users should regularly backup the SQL database. The interval between backups defines the maximum time window over which data would be lost. Typical installations would perform full nightly backups of the database. Please see the Section 0 Backup and Recovery of the TMS database for details on how to perform backups and restores of the database. The secondary SQL server does not need to be backed up explicitly as it is always updated from the primary SQL server.

Customer files must be synchronized between Cisco TMS servers as discussed in the installation section. Please see Section 0 Customer specific TMS Files

for details.

Upgrading TMS

All Cisco TMS servers accessing the same database must be running the same Cisco TMS version. When upgrading between Cisco TMS versions, there will be inconsistencies between different servers as each is upgraded so extra steps are required when performing Cisco TMS upgrades or patches.

These steps assume you are only using one Cisco TMS server in both the primary and off-site locations. You may combine this model with other Cisco TMS deployment models such as using a Network Load Balancer with multiple Cisco TMS servers in each location. The instructions for upgrading such a scenario will not be documented here, but would follow the same methods where you would use the upgrade steps outlined in previous sections within each site. It is critical that the off-site location must be completely disabled, all Cisco TMS services and websites after the upgrade, until the off-site location is activated to become the primary site.

When performing a Cisco TMS upgrade, the following steps must be followed

- Plan an upgrade during a time window when Cisco TMS can be made unavailable to users as Cisco TMS will be unavailable during the duration of your upgrade
- Log into the Windows console the primary Cisco TMS server, and from the Services component of Computer Management, manually stop all services whose name starts with Cisco TMS and the WWWPublishingSevice service. The off-site Cisco TMS server should already be stopped but verify before proceeding.
- Start on the primary Cisco TMS server. Start the installer for the Cisco TMS upgrade as normal. During this process, any updates to the SQL database will be performed.
- The installer will likely restart the Cisco TMS services and WWWPublishingService and may require a reboot of the server. After the reboot, go into Services component of Computer Management, manually stop all services whose name starts with Cisco TMS and the WWWPublishingService
- Force a replication of the tmsng database to the off-site SQL server. Wait for the off-site SQL server to complete its update before proceeding.

- Log into the Windows console of the off-site Cisco TMS server and start the upgrade or patch installer the same as you did on the first Cisco TMS server. The installer will likely restart the Cisco TMS services and WWWPublishingService and may require a reboot of the server. After the reboot, go into Services component of Computer Management, manually stop all services whose name starts with Cisco TMS and the WWWPublishingService. The services may also be configured for automatic startup. Right-click on each of these services and select Properties. On the General tab of each of the services you stopped, set startup type to Manual.
- If your deployment model has multiple servers, follow the steps for upgrading Cisco TMS per the relevant section of this document.
- Once the off-site location has been upgraded, log into the Windows console of the primary server and restart all Cisco TMS services and WWWPublishingService service. Your upgrade is now complete.

Model Summary

Immediate fail-over available.
Not for primary to secondary site, but possible to have automatic failover within a location.

Amount of data lost.
The intervals defined in your Log shipping configuration dictates out of date the secondary SQL server is. Activity on the primary server since the last log shipment would be lost in a fail-over.

Time to restore service.
Variable on how long it would take to reconfigure devices and start-up the secondary server. Estimate a half hour or more to activate the secondary site and update configurations to point to the new secondary site.

Administrative Capabilities Required
High for configuring SQL Log Shipping and Managing cut-over to secondary site.

Cost.
High. Must implement multiple servers in multiple locations.

Customer specific TMS Files

Part of the Cisco TMS installation will consist of files added or customized by users and administrators. These files will consist of software and images uploaded to Cisco TMS, images created by Cisco TMS, and any templates that may be customized by an administrator. These files will vary from a default installation so they must be backed up to perform a complete server restore. In addition, when using multiple Cisco TMS servers, these files must be synchronized between the different servers.

These files are located in the following directories in a default installation:

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\CiscoSettings

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\CompanyLogo

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\EmailTemplate

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\image

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\Logo

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\Map

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\MGCSettings

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\Software

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\Sound

All of these directories should be backed up as part of a regular back-up schedule in addition to the Cisco TMS database, tmsng on the SQL Server.

To restore a Cisco TMS installation without requiring a complete server recovery, Cisco TMS can be freshly installed from installation media and then restore the customer specific information. The customer specific information includes the Cisco TMS database and the data files listed above. Restoring the Cisco TMS database is covered in Section 0 Backup and Recovery of the TMS database. Restoring the Cisco TMS customer specific files means simply restoring the directories listed above from backup to their original location after completing the Cisco TMS installation. These files combined with the Cisco TMS database will take a fresh installation of Cisco TMS fully back to the backup point.

TMS Customer file synchronization

When using multiple Cisco TMS servers, the directories containing the customer specific files are not automatically shared between the different Cisco TMS servers. For full functionality, these files must be synchronized between the Cisco TMS servers. These files consist of:

- administrator modified Cisco TMS email templates
- administrator modified MCU templates (for Cisco/Rad/MGC MCUs)
- user uploaded logos/graphics (templates and Cisco TMS logo)
- user uploaded images for Map Monitor
- user uploaded software files

These files need to be synchronized between all Cisco TMS servers for full seamless functionality. The directories that must be synchronized are:

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\CiscoSettings

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\CompanyLogo

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\EmailTemplate

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\image

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\Logo

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\Map

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\MGCSettings

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\Software

c:\program files\TANDBERG\TMS\wwwCisco TMS\Data\Sound

These files may be synchronized using any method or tools an administrator chooses. An important note is the overwriting of files. Some of these files when updated would have the same name as files on another server. Your synchronization process must take into account which file should be the one to keep vs. overwriting. This is most critical if you change the email templates or MCU settings templates. A simple method to address this is to have one server be considered the 'master' and when updating these template files, have these files overwrite all other copies. Any changes to these files must be done on the master server. This concern only applies to files that will have duplicate file names.

A simple example to show how to copy files from one server to another using the built-in utilities of Windows is shown below. This script can be saved as a batch file and creating a scheduled job to run it automatically. Create a text file with the following lines, and save as c:\SyncCisco TMSData.bat . The variables Cisco TMS_DATA_ROOT_SOURCE and Cisco TMS_DATA_ROOT_DEST should be updated based on your Cisco TMS installation's details

```
SET TMS_DATA_ROOT_SOURCE=c:\program files\TANDBERG\TMS\wwwTMS\Data
SET TMS_DATA_ROOT_DEST=\\TMSServer2\c$\program
files\TANDBERG\TMS\wwwTMS\Data

xcopy "%TMS_DATA_ROOT_SOURCE%\CiscoSettings\*"
"%TMS_DATA_ROOT_DEST%\CiscoSettings\" /D
xcopy "%TMS_DATA_ROOT_SOURCE%\CompanyLogo\*"
"%TMS_DATA_ROOT_DEST%\CompanyLogo\" /D
xcopy "%TMS_DATA_ROOT_SOURCE%\EmailTemplate\*"
"%TMS_DATA_ROOT_DEST%\EmailTemplate\" /D
xcopy "%TMS_DATA_ROOT_SOURCE%\Image\*" "%TMS_DATA_ROOT_DEST%\Image\" /D
xcopy "%TMS_DATA_ROOT_SOURCE%\Logo\*" "%TMS_DATA_ROOT_DEST%\Logo\" /D
xcopy "%TMS_DATA_ROOT_SOURCE%\Map\*" "%TMS_DATA_ROOT_DEST%\Map\" /D
xcopy "%TMS_DATA_ROOT_SOURCE%\MGCSettings\*"
"%TMS_DATA_ROOT_DEST%\MGCSettings\" /D
xcopy "%TMS_DATA_ROOT_SOURCE%\Software\*" "%TMS_DATA_ROOT_DEST%\Software\"
/D
xcopy "%TMS_DATA_ROOT_SOURCE%\Sound\*" "%TMS_DATA_ROOT_DEST%\Sound\" /D
```

Using the 'at' program, the batch file can be ran daily automatically. Use the following command at the command prompt to schedule the job

```
at 23:00 /EVERY:m,t,w,th,f,s,su c:\SyncTMSData.bat
```

These files do not change very often, so synchronization does not have to run at a high frequency. A best practice would be to run an update at most once an hour. The above script illustrates how to copy files from one server to another. To complete the synchronization, files must be copied from the other server back to the first as well, to make sure both servers have all files that may have originated on the other server.

Backup and Recovery of the TMS database

Cisco TMS utilizes a standard Microsoft SQL database and server, so any compatible SQL tools may be used to backup and recover the database. The database can be backed up at any time without interrupting Cisco TMS service, but the database can not be in use when performing a database restore. If any Cisco TMS service or website is running, the database will be in use and you will not be able to restore the database. The database created by Cisco TMS is named tmsng. Backing up and restoring the database is the same for all Cisco TMS deployment models as there will always only be one active database in any Cisco TMS installation.

Microsoft reference for backing up and restoring SQL databases

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/architec/8_ar_aa_9iw5.asp

Using osql to manage databases

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/acdata/ac_8_mta_01_7apd.asp

Backing up the database

The database can be backed up using any Microsoft SQL utility, including Enterprise Manager, osql, or any 3rd party SQL backup agent. To simplify the process, Cisco TelePresence also provides a utility to perform SQL backups or restores. The Database management utility can be installed on the Database server, or on another computer that can connect to the database remotely. The Database Utility provides a graphical interface to specify the database server, and backup the database. The utility can also perform backups automatically on a scheduled basis.

A default method available for any Microsoft SQL server will be using osql, the command line SQL client. The database created for Cisco TMS is named tmsng. To create a backup of the Cisco TMS database on a SQL server named ACME\WIDGETS named tmsbackup.bak in c:\, enter the following command in a command window on the database server

```
osql –U sa –S ACME\WIDGETS –Q “backup database tmsng to disk =
‘c:\tmsbackup.bak’”
```

You will be prompted for the password to the sa account and then the backup will execute.

Note: If the SQL server is installed as a named instance or part of a cluster, you will have to specify the SQL server name or address in the osql command as shown in the example. If the server is the default instance, you can omit the –S option and server name.

Restoring the TMS Database

The database can be restored using any Microsoft SQL utility, including Enterprise Manager, osql, or any 3rd party SQL utility. To simplify the process, Cisco TelePresence also provides a utility to perform SQL backups or restores. The database can not be in use while performing a restore. So before any restore can be done the Cisco TMS services and website must be stopped. Before any restore, perform the following steps

- Log into the Windows console of the Cisco TMS Server and open Computer Management under Administrative Tools
- Under Services, stop all services who’s name begins with Cisco TMS and the WWWPublishingService
- Repeat these steps for all Cisco TMS Servers pointing at the database to be restored
- Once the database restore is complete, the services that were stopped can be restarted by following the same steps and selecting start.

The Database management utility can be installed on the Database server, or on another computer that can connect to the database remotely. The Database Utility provides a graphical interface to specify the database server, and restore the database.

A default method available for any Microsoft SQL server will be using osql, the command line SQL client. The database created for Cisco TMS is named tmsng. To restore the Cisco TMS database on a

SQL server named ACME\WIDGETS from a backup file c:\tmsbackup.bak enter the following command in a command window on the database server

```
osql –U sa –S ACME\WIDGETS –Q “restore database tmsng from disk =
‘c:\tmsbackup.bak’”
```

You will be prompted for the password to the sa account and then the restore will execute.

Note: If the SQL server is installed as a named instance or part of a cluster, you will have to specify the SQL server name or address in the osql command as shown in the example. If the server is the default instance, you can omit the –S option and server name.

A database named tmsng must exist on the SQL server before you can restore from a backup

A database backup includes the file paths used for the database. If for some reason the database files are in a different location from when the backup was taken, you must use the MOVE options with the restore commands. Please see the Microsoft SQL documentation for help using the MOVE option.

Cisco TMS Redundancy limitations and notes

This section will outline functionalities that may be affected or operate differently when using Cisco TMS in a redundant fashion.

Event Execution

- Events that have already begun to execute by a particular server will not be completed by another server if the executing server fails.
  Events can be executed by any Cisco TMS server connected to the database. Once an event starts on a particular server, it will not be resumed by another server. So if a server fails, any actively executing events on that server will potentially not complete. This only affects events that are in progress. As most evens finish very quickly, the number of concurrently running events on a server should be low, so the number of potential events affected by a server failure will be low .
  Some examples of events that can be affected:
  - A software upgrade in mid-progress will fail if the server running the event fails.
  - A template push to systems will fail if the server running the event fails.

Conference Connection and Control

Execution of scheduled calls in Cisco TMS is actually broken into three phases. Initiation, Active Monitoring, and Disconnection. Initiation and Disconnection are actually handled as separate events for resiliency. Active Monitoring will be handled by the Cisco TMS Server who handled the call initialization. By default, the same Cisco TMS server that was used to book a call will be the default to execute the call and all phases of the call. If a server fails, there are limitations to how active calls being handled by that server will be handled. Calls that have not begun the initialization phase or are executing on other servers will not be affected.

- Automatic call launch.
  If the primary Cisco TMS server for call launching is not active, another active Cisco TMS server will start the conference after 60 seconds. If no secondary server is running when the call is scheduled to start, a check is made when a server does come up for any call that has not started that should have been and will start them
- Conferences that are still initializing and have not finished connecting will not automatically be started.
  15 minutes prior to a conference's scheduled start time, a conference will be initialized by one server. If that Cisco TMS server fails before the conference finishes being connected, the conference will not be connected by another Cisco TMS server.
- Conferences that are in the process of being disconnected may fail to completely disconnect.
- If the server performing the conference disconnection fails during the actual disconnection of the conference, the conference may not automatically be ended.