Cisco TelePresence Management Suite Redundancy

Deployment Guide

Version 13.2

D14570.04

September 2012

Contents

Introduction

Cisco TMS supports deployment in a redundant configuration, increasing the availability of the application.

Understanding how Cisco TMS communicates with managed systems is key to understanding Cisco TMS redundancy. This is explained in the first section of the document.

This document also describes the requirements, configuration, and limitations of deploying Cisco TMS in the two supported redundant scenarios:

- For a fully redundant Cisco TMS deployment with an automatic failover process, you must set up two Cisco TMS servers with a network load balancer (NLB) in front. Cisco recommends using a Cisco ACE 4710 Application Control Engine Appliance for load-balancing IP traffic between the two Cisco TMS servers, therefore this document describes how to deploy Cisco TMS with an ACE 4710 appliance.
- This document also describes how to deploy two Cisco TMS servers using a Hot Standby model.

It is assumed that the reader has an understanding of Cisco TMS, Cisco TMS installation, and Windows Server operating systems, as well as an advanced level of understanding of computer networking and network protocols.

Supported configurations

Regardless of which of the two redundancy models you choose to deploy, no more than two Cisco TMS servers can be used. Deploying more than two Cisco TMS servers in a redundant setup is neither tested nor supported by Cisco.

Deploying two Cisco TMS servers will increase Cisco TMS availability, but will not in any way increase Cisco TMS scalability.

Other models of load balancer with alternative configurations may work with Cisco TMS, but have not been tested by Cisco.

Licensing

Only one live database can be used in a redundant Cisco TMS implementation, therefore both servers will use the same Cisco TMS serial number and the same set of release and option keys.

Database redundancy

Cisco TMS relies heavily on its SQL database, so a fully resilient Cisco TMS solution will also utilize one of the high-availability technologies offered by SQL Server 2008. Thoroughly documenting SQL Server 2008 high-availability alternatives is beyond the scope of this document, but the two relevant SQL Server redundancy models are briefly discussed in the Database redundancy [p.19] section of this document along with references to the relevant Microsoft documentation.

Cisco TMS Provisioning Extension and redundancy

Implementing Cisco TMSPE in a redundant environment is described in the Cisco TelePresence Management Suite Provisioning Extension Deployment Guide.

Understanding how Cisco TMS communicates with managed systems

Cisco TMS uses HTTP/HTTPS when communicating with managed endpoints and infrastructure products. In addition, SNMP and FTP are used for communicating with some older endpoints, such as the Cisco TelePresence System MXP series.

Managed systems also initiate connections to Cisco TMS. Examples of such connections include phonebook requests, boot and registration events, and heartbeats from SOHO systems. Each Cisco TMS-managed system must therefore be configured with an External Manager Address, which is used for contacting Cisco TMS.

The addresses that systems use to contact Cisco TMS

You specify addresses that systems use for contacting Cisco TMS by going to **Administrative Tools > Configuration > Network Settings**.

- The IPv4, IPv6, and Fully Qualified Host Name addresses specified in the **Advanced Network Settings for Systems on Internal LAN** are used by systems that have their **System Connectivity** status set to *Reachable on LAN*.
- The Fully Qualified Host Name or IPv4 address specified in **Advanced Network Settings for Systems on Public Internet/Behind Firewall** is used by systems that have their **System Connectivity** status set to *Reachable on Public Internet* or *Behind Firewall*.

System Connectivity status

The **System Connectivity** status is configurable when an administrator adds a system to Cisco TMS or at a later time by going to **Systems > Navigator >** select a system **> Connection** tab **> System Connectivity** in Cisco TMS. By default systems are set to *Reachable on LAN*.

If the **Enforce Management Settings on Systems** setting is set to *Yes* in **Administrative Tools > Network Settings > TMS Services**, Cisco TMS periodically pushes server information to systems:

- The Fully Qualified Host Name (if set) or the IP address (if the Fully Qualified Host Name is not set) is pushed to systems with **System Connectivity** status set to *Reachable on LAN*.
- The **TMS Server Address (Fully Qualified Host Name or IPv4 Address)** setting is pushed to systems with **System Connectivity** status set to *Reachable on Public Internet*.

The third **System Connectivity** option used by Cisco TMS is *Behind Firewall*. Cisco TMS assumes that systems set to *Behind Firewall* are located behind a firewall or a router that uses network address translation (NAT). Cisco TMS is then unable to connect to the system, for example to instruct it to launch a call. Having a system set to *Behind Firewall* status will severely limit what you can do with the system in Cisco TMS.

Why Cisco TMS changes the System Connectivity status

Cisco TMS will in some cases change the **System Connectivity** status based on boot and registration events sent by a system.

Whenever a system sends a boot or registration event, Cisco TMS compares the reported IP address with the HTTP header's source IP address.

Here is an example registration event sent to Cisco TMS from a Cisco TelePresence System Integrator C Series system:

```
(...)
<PostEvent>
       <Identification>
              <SystemName>example_system</SystemName>
              <MACAddress>A1:B2:C3:D4:E5:F6</MACAddress>
              <IPAddress>172.16.0.20</IPAddress>
              <ProductType>TANDBERG Codec</ProductType>
              <ProductID>TANDBERG Codec</ProductID>
              <SWVersion>TC4.1.2.257695</SWVersion>
              <HWBoard>101400-5 [08]</HWBoard>
              <SerialNumber>B1AC00A00000</SerialNumber>
       </Identification>
       <Event>Register</Event>
</PostEvent>
(...)
```

In the example above, the Cisco TelePresence Codec C90 reports its local IP address as: 172.16.0.20.

- If these two IP addresses are the same, Cisco TMS keeps the **System Connectivity** status the same as it was when the system was originally added to Cisco TMS.
- If the two IP addresses are not the same, Cisco TMS will try to contact the system on the IP address in the HTTP header:
  - If the system then responds to requests sent to this address, Cisco TMS sets the **System Connectivity** to either *Reachable on LAN* or *Reachable on Public Internet*. It compares the address the system used to reach Cisco TMS with the DNS addresses set in **Advanced Network Settings for Systems on Internal LAN > TMS Server Fully Qualified Host Name** and **Advanced Network Settings for Systems on Public Internet/Behind Firewall > TMS Server Address (Fully Qualified Host Name or IPv4 Address)** in the Cisco TMS application:
    - If the address used by the system is equal to the internal address (or to both, if both addresses are set to the same DNS name) the system is set to *Reachable on LAN*.
    - If the address is equal to the public address only, the system is set to *Reachable on Public Internet*.
  - If the system does not respond to the request sent to the IP address from the HTTP header, Cisco TMS changes its **System Connectivity** status to *Behind Firewall*.

Examples

- A system is set to *Reachable on LAN*, and reports its IP address as: 172.16.0.20. The IP source address in the HTTP header is also: 172.16.0.20. Cisco TMS keeps the system as *Reachable on LAN*.
- A system is set to *Reachable on LAN*, and reports its IP address as: 172.16.0.20. The IP source address in the HTTP header is: 10.0.0.50. Cisco TMS then attempts to contact the system on 10.0.0.50. When the request times out, Cisco TMS changes the system to *Behind Firewall*.
- A system is set to *Reachable on Public Internet*, and reports its IP address as: 172.16.0.20. The IP source address in the HTTP header is: 10.0.0.50. Cisco TMS then attempts to contact the system on 10.0.0.50, and the network device at 10.0.0.50 is able to route the traffic back to the original system. The original system replies to Cisco TMS, and Cisco TMS keeps the system as *Reachable on Public Internet*.

Network load balancer deployment

When deploying two Cisco TMS servers behind a load balancer such as the Cisco ACE 4710 Application Control Engine Appliance, one virtual IP address must be assigned to the NLB and one IP address assigned

to each of the two Cisco TMS servers.

A DNS entry must be created pointing to the NLB's virtual IP address.

The NLB's host name and IP address(es) must be entered in the fields on the **Network Settings** page in Cisco TMS discussed in The addresses that systems use to contact Cisco TMS [p.5] above.

See Deploying with a load balancer [p.8] for instructions on implementing this configuration.

Once the IP addresses and host name values in **Network Settings** have been changed, the Database Scanner service enforces the new network settings on the managed systems. The systems then start directing traffic to the NLB, which forwards the requests to the Cisco TMS servers.

All communication between Cisco TMS and the managed systems will now go through the NLB. This is accomplished by keeping the Cisco TMS servers and the managed systems on different VLANs while the servers use the NLB as their default gateway.

Cisco TMS's logic for determining whether a system is *Reachable on LAN*, *Reachable on Public Internet* or *Behind Firewall* dictates how you set up the load balancer. As it is limiting to have systems in a *Behind Firewall* status, the load balancer must be configured so that all traffic from managed systems appears to Cisco TMS as coming directly from the managed systems and not from the NLB.

Deploying with a load balancer

Configuring two Cisco TMS servers (also referred to as "nodes" in this context) with a network load balancer (NLB) provides a truly redundant Cisco TMS setup with fully automatic fail-over.

This deployment can be combined with a high-availability SQL Server option as discussed in the Database redundancy [p.19] section.

Requests from the systems managed by Cisco TMS pass transparently through the NLB so that the traffic appears to come directly from the managed systems. (See Understanding how Cisco TMS communicates with managed systems [p.5])

Recommended hardware

We recommend using the Cisco ACE 4710 Application Control Engine Appliance. The ACE is the only load balancer that has been tested and verified to work with Cisco TMS.

Fully documenting how to set up and manage an ACE appliance is outside the scope of this document, but a sample configuration document showing a Cisco TMS-compatible ACE configuration has been included in Appendix 1. Example ACE configuration [p.21] for your reference.

(See the Cisco ACE 4700 Series Application Control Engine Appliance documentation for further information.)

Active directory and user authentication requirements

- Both Cisco TMS servers must be members of the same Windows domain.
- All Cisco TMS users must be imported from and authenticated using Active Directory.
- Using local user accounts is not supported for this redundancy model.

Architectural overview and network diagram

Example configuration

In the example below the following values are used:

VLAN200

Device	IP address	Hostname
ACE Virtual IP	10.0.200.40	tms.example.com
tms01	10.0.200.50	tms01.example.com
tms02	10.0.200.60	tms02.example.com
SQL Server	10.0.200.70	sql01.example.com

VLAN100

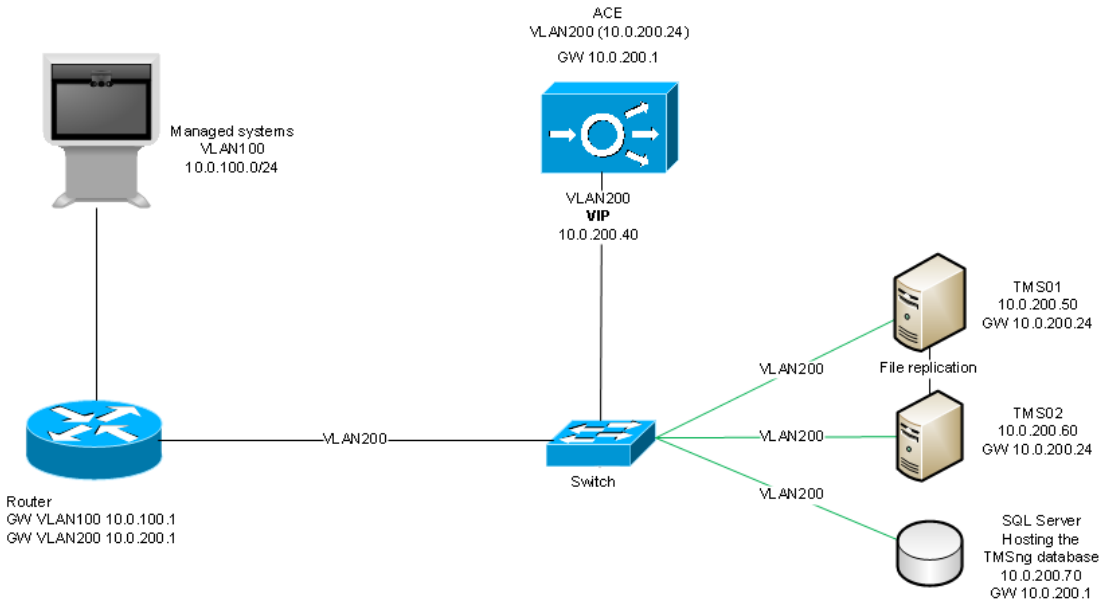
Device	IP address	Hostname
Managed systems and users	10.0.100.0/24	

- There are two Virtual LANs, VLAN200 and VLAN100.
- The ACE is configured on VLAN200.
- The two Cisco TMS servers (tms01 at 10.0.200.50 and tms02 at 10.0.200.60) are configured on VLAN200.
- All clients (managed systems and users) are configured on VLAN100. Clients must not be on the same VLAN as the load balanced Cisco TMS servers.
- All traffic to the virtual IP address of the ACE is forwarded to one of the two Cisco TMS servers.
- All managed systems and users use the ACE's virtual IP address when communicating with Cisco TMS.
- The default gateway of both Cisco TMS servers is set to the ACE's IP address on VLAN200 to ensure that all traffic to and from Cisco TMS is load balanced.

Database

- The two Cisco TMS servers share a common, external tmsng database.
- As both Cisco TMS servers simultaneously read and write data to the database the server hosting SQL Server needs more powerful hardware than if it only served one Cisco TMS server.
- The database server talks directly to the Cisco TMS servers, bypassing the ACE load balancer.

Transparent Source Network Address Translation



Installing and configuring

Installing Cisco TMS on tms01

1. Prior to installing Cisco TMS, set up an SQL Server instance on an external server.
2. Install Cisco TMS on the first node, using the instructions provided in the Cisco TelePresence Management Suite Installation and Getting Started Guide.
3. Use the "Custom" installation mode, and point Cisco TMS to the external database server.

4. If enabling HTTPS during installation, use a certificate issued to tms.example.com.
5. After the server has rebooted, log in to the Cisco TMS web application to verify that it works correctly.

Installing Cisco TMS on tms02

1. Check that the operating system including service pack level on tms02 is exactly the same as on tms01.
2. Check that both servers are configured with the same time zone.
3. Install Cisco TMS using the same external database server and installation directory as when setting up tms01. Install the same version of Cisco TMS.
4. If HTTPS was enabled during installation on tms01, use the same certificate used on tms01.
5. After the server has rebooted, log in to the Cisco TMS web application to verify that it works correctly.

Setting up the network load balancer

Once the second node is operational, set up the network load balancer. For the Cisco ACE 4710 Application Control Engine Appliance, this includes configuring:

- Virtual Servers
- Real Servers
- Server Farms
- Health Monitoring
- Stickiness

See Appendix 1. Example ACE configuration [p.21] for a reference ACE configuration.

Configuring Cisco TMS

On one of the nodes:

1. In the Cisco TMS application go to **Administrative Tools > Configuration > Network Settings**.
2. Change the following IP address(es) and host names to the NLB's virtual IP address(es) and host name:
   - **Event Notification > SNMP Traphost IP Address**
   - **Advanced Network Settings for Systems on Internal LAN**: all fields
   - **Advanced Network Settings for Systems on Public Internet/Behind Firewall**

On both nodes:

1. Go to **Control Panel** on the Windows server.
2. In **Network Settings** change the default gateway to be the NLB's IP address.
3. Verify that the Cisco TMS servers can reach the managed systems and vice versa.

Synchronizing local files

Some customizable files used by Cisco TMS are stored in the Windows server's local file system rather than in the tmsng database. The folders these files are stored in must be kept synchronized between the two nodes. See Appendix 2. Local files for synchronization [p.25] for a full list of the folders that must be synchronized.

Use your preferred method of synchronizing the folders; for example you could create a shell script that uses xcopy/robocopy to copy files between the two nodes.

The network load balancer, protocols and probes

HTTP/HTTPS/SNMP: Sticky connections

Configure the NLB to forward HTTP and HTTPS connections as well as SNMP traps to the Cisco TMS servers using sticky connections.

Using sticky connections ensures that new connections from a client IP address are assigned to the same Cisco TMS node that received previous connections from that address.

Traffic must be forwarded to one single server, not both servers.

Other protocols

Other protocols such as SSH and FTP are always initiated from the Cisco TMS side. No special configuration of the NLB is required for these protocols.

Probes

A probe is a request sent from the NLB to a node to check whether a particular service is still responding.

Whenever a probe fails, the load balancer, assuming that the node is at least partially inoperative, directs all traffic to the other node and notifies the network administrator.

We recommend probing:

- TMS Scheduler (/tms/booking)
- Cisco TMS web application (/tms)

Create a new domain service account specifically for probing.

This service account does not need any specific rights in Cisco TMS itself and can be a member of the “Users” group only. It must, however, be allowed by IIS to authenticate and log in to Cisco TMS.

See Appendix 1. Example ACE configuration [p.21] for a sample configuration.

Scheduled tasks

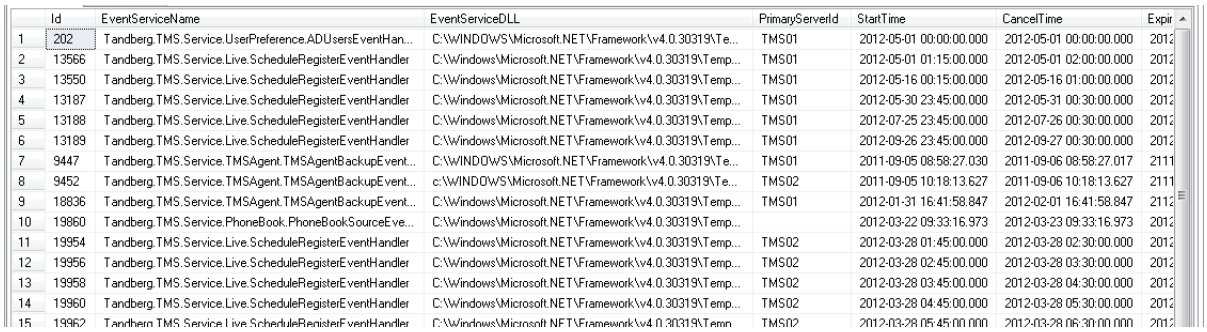
Some tasks in Cisco TMS are scheduled.

Examples include:

- Updating phone book sources from gatekeeper registration lists
- Pushing configuration templates to managed systems
- Mirroring user directories

Such tasks are assigned randomly to one of the two Cisco TMS nodes.

To see which node has been assigned a task, go to the PrimaryServerId column of the SchedulerEvent table in the tmsng database:



	Id	EventServiceName	EventServiceDLL	PrimaryServerId	StartTime	CancelTime	Expir
1	202	Tandberg.TMS.Service.UserPreference.ADUsersEventHan...	C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\Te...	TMS01	2012-05-01 00:00:00.000	2012-05-01 00:00:00.000	2012
2	13566	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS01	2012-05-01 01:15:00.000	2012-05-01 02:00:00.000	2012
3	13550	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS01	2012-05-16 00:15:00.000	2012-05-16 01:00:00.000	2012
4	13187	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS01	2012-05-30 23:45:00.000	2012-05-31 00:30:00.000	2012
5	13188	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS01	2012-07-25 23:45:00.000	2012-07-26 00:30:00.000	2012
6	13189	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS01	2012-09-26 23:45:00.000	2012-09-27 00:30:00.000	2012
7	9447	Tandberg.TMS.Service.TMSAgent.TMSAgentBackupEvent...	C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\Te...	TMS01	2011-09-05 08:58:27.030	2011-09-06 08:58:27.017	2111
8	9452	Tandberg.TMS.Service.TMSAgent.TMSAgentBackupEvent...	c:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\Te...	TMS02	2011-09-05 10:18:13.627	2011-09-06 10:18:13.627	2111
9	18836	Tandberg.TMS.Service.TMSAgent.TMSAgentBackupEvent...	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS01	2012-01-31 16:41:58.847	2012-02-01 16:41:58.847	2112
10	19860	Tandberg.TMS.Service.PhoneBook.PhoneBookSourceEve...	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...		2012-03-22 09:33:16.973	2012-03-23 09:33:16.973	2012
11	19954	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS02	2012-03-28 01:45:00.000	2012-03-28 02:30:00.000	2012
12	19956	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS02	2012-03-28 02:45:00.000	2012-03-28 03:30:00.000	2012
13	19958	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS02	2012-03-28 03:45:00.000	2012-03-28 04:30:00.000	2012
14	19960	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS02	2012-03-28 04:45:00.000	2012-03-28 05:30:00.000	2012
15	19962	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS02	2012-03-28 05:45:00.000	2012-03-28 06:30:00.000	2012

- If the PrimaryServerId field for a given task is empty, the task will be executed by the first node that polls the database for tasks after the task is scheduled to start.
- If the PrimaryServerId field for a given task shows a node that is operational, that node will pick up the task as soon as the task is scheduled to start.
- If the PrimaryServerId field for a given task shows a node that is not operational, the other node will pick up the task after 60 seconds and execute it.

Cisco TMS does not directly assign tasks to nodes based on server load. The other node picks up a task if the original node is under such a heavy load that it is unable to poll the database for new tasks—this offers a similar balancing mechanism.

The other node will not pick up and re-execute the task if the original assignee fails during execution of that task.

Live Service and the Conference Control Center

When a conference is booked in Cisco TMS, it is allocated to the Live Service on one of the two nodes. The Live Service collects data about the conference, which will display in **Monitoring > Conference Control Center** in Cisco TMS.

If a conference is owned by the Live Service on tms01, but the load balancer forwards feedback from one of the participants in the conference to tms02, tms02 uses a remote procedure call (RPC) to pass the information to tms01.

If a user logged on to tms01 makes a change to an ongoing conference owned by tms02 in **Conference Control Center** (CCC):

1. Tms01 sends the change to tms02 using RPC.
2. Tms02's Live Service then instructs the systems involved to make the change.

Live Service uses TCP port 8085 for RPC. If changes made in CCC are slow to propagate from one node to the other:

1. Check that a firewall is not blocking traffic on port 8085.
2. Verify that both Cisco TMS servers are listening on port 8085:
   - Open a cmd shell and execute a `netstat -a -n | findstr :8085` command on both servers
   - Try to connect using telnet (`telnet tms01.example.com 8085`) and check that the connections are not refused .

To check which node owns an ongoing conference and its participants, see the RunningServer column of the LiveStatusData table in the tmsng database. This field contains either "tms01" or "tms02".

	ConferenceId	CallId	StatusText	RunningServer	TimeStamp	Type
1	1321	SYSTEM:2:123	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS02	2012-05-04 09:34:51.967	3
2	1321	SYSTEM:1:49	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS02	2012-05-04 09:34:13.967	3
3	1321	SYSTEM:1:103	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS02	2012-05-04 09:34:21.660	3
4	1321	SYSTEM:1:102	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS02	2012-05-04 09:34:21.647	3
5	1321	CONF	<?xml version="1.0" encoding="utf-8"?><LiveConfe...	TMS02	2012-05-04 09:34:21.660	1
6	1321	2:123MCU-1:49Endpoint	<?xml version="1.0" encoding="utf-8"?><LiveCallD...	TMS02	2012-05-04 09:34:25.977	2
7	1321	2:123MCU-1:103Endpoint	<?xml version="1.0" encoding="utf-8"?><LiveCallD...	TMS02	2012-05-04 09:34:25.970	2
8	1321	2:123MCU-1:102Endpoint	<?xml version="1.0" encoding="utf-8"?><LiveCallD...	TMS02	2012-05-04 09:34:25.973	2
9	1305	SYSTEM:2:127	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-02 11:56:35.607	3
10	1305	CONF	<?xml version="1.0" encoding="utf-8"?><LiveConfe...	TMS01	2012-05-04 09:33:42.323	1
11	1304	SYSTEM:2:127	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-02 11:56:35.603	3
12	1304	CONF	<?xml version="1.0" encoding="utf-8"?><LiveConfe...	TMS01	2012-05-04 09:33:42.330	1
13	1303	SYSTEM:2:127	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-02 11:56:35.603	3
14	1303	CONF	<?xml version="1.0" encoding="utf-8"?><LiveConfe...	TMS01	2012-05-04 09:33:42.330	1
15	1302	SYSTEM:2:127	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-03 15:08:17.370	3
16	1302	SYSTEM:15:130202	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-03 15:51:01.880	3
17	1302	SYSTEM:15:130201	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-03 15:13:58.577	3
18	1302	SYSTEM:15:130200	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-03 15:08:17.367	3
19	1302	CONF	<?xml version="1.0" encoding="utf-8"?><LiveConfe...	TMS01	2012-05-04 09:33:42.327	1
20	1301	SYSTEM:2:127	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-02 11:56:35.610	3
21	1301	CONF	<?xml version="1.0" encoding="utf-8"?><LiveConfe...	TMS01	2012-05-04 09:33:42.337	1

Conferences that are scheduled to start more than 15 minutes into the future are stored in the SchedulerEvent table as described in the Scheduled tasks [p.11] section above. You can then see which node will control the conference by examining the PrimaryServerId value.

Conferences scheduled to start less than 15 minutes into the future are not written to the SchedulerEvent table, but are directly assigned to the Live Service on the node the conference was scheduled on.

Upgrading Cisco TMS

Upgrading Cisco TMS to a later software version must be done during a maintenance window, as upgrading will make Cisco TMS unavailable to users for a short period of time.

As the two Cisco TMS nodes share a common database, they must run the same software version at all times. It is therefore not possible to upgrade one node at a time and keep the other node operational to serve systems and users.

1. Log in to both Cisco TMS Windows servers.
2. Stop all the TMS services, as well as the IIS service on both nodes.
3. Upgrade one of the nodes to the new software version. This will upgrade the tmsng database.
4. Log in to the Cisco TMS web application on this server to verify that it works correctly.

The probes on the NLB will now report that only the first Cisco TMS server is operational so all traffic will automatically be directed to this node. Users and managed systems can now use Cisco TMS again.

1. Upgrade the second Cisco TMS node.
2. The installer will detect that the database has already been upgraded, and offer to continue using the updated database: select **Yes**. The installer will then update the binaries and leave the database alone.
3. Log in to the Cisco TMS web application on this server to verify that it works correctly.

Check that the network settings have not been changed during the install process:

1. In the Cisco TMS application go to **Administrative Tools > Configuration > Network Settings**.
2. Check that the following IP address(es) and host names are set to the NLB's virtual IP address(es) and host name:
   - **Event Notification > SNMP Traphost IP Address**
   - **Advanced Network Settings for Systems on Internal LAN**: all fields
   - **Advanced Network Settings for Systems on Public Internet/Behind Firewall**

Recovery in case of a failing node

No immediate action is required in the event of a server failure, as the NLB will automatically detect the failure and direct all traffic to the other node.

Troubleshoot the failing node's software and hardware as you normally would, and bring it back online once it is operational.

The NLB will detect that the node is up again and traffic will then be forwarded to both nodes as normal.

Deploying a hot standby

Keeping an additional Cisco TMS server as a warm spare in case of failure is known as the "Hot Standby" redundancy model.This requires manual intervention if there is a failure on the primary Cisco TMS server, and is therefore a switchover solution rather than a failover solution.

One Cisco TMS server is active at any given time with this redundancy model. The hot standby server must be kept up to date with security patches and other upgrades so that it is ready for activation within a few minutes if the primary server fails.

Note that the hot standby redundancy model requires the tmsng database to be located on an external SQL server, and that the two Cisco TMS servers must be in the same Windows domain.

In the instructions below the following examples are used:

Server	DNS Name	IP Address
Primary Cisco TMS Server (tms01)	tms01.example.com	10.0.0.10
Secondary Cisco TMS Server (tms02)	tms02.example.com	10.0.0.11

The examples assume that you use IPv4. If you also use IPv6, change the IPv6 addresses accordingly.

Setting up the primary Cisco TMS server

Prior to installing Cisco TMS:

1. Set up an SQL server instance on an external server.
2. Set up a DNS entry: tms.example.com pointing to the IP address of the primary server tms01 (10.0.0.10).
3. Install Cisco TMS on tms01 using the instructions provided in the Cisco TMS Installation and Getting Started Guide, but:
   a. Use the "Custom" installation mode.
   b. Point Cisco TMS to the external database server you used in step 1.
4. If enabling HTTPS during installation, use a certificate issued to tms.example.com.
5. After the server has rebooted, log in to the Cisco TMS web application to verify that it works correctly.

All users and managed systems must use tms.example.com when connecting to Cisco TMS. The server's own hostname (tms01.example.com) must not be used.

After verifying that the installation of Cisco TMS was successful:

1. In Cisco TMS go to **Administrative Tools > Configuration > Network Settings**.
2. Enter *tms.example.com* in the **TMS Server Fully Qualified Host Name** and **TMS Server Address (Fully Qualified Host Name or IPv4 Address)** fields.

Do not use local user accounts when logging in to Cisco TMS. All user accounts must be domain accounts, so that they are available if you have to swap to the secondary server, tms02.

Setting up the secondary Cisco TMS server

1. Check that the operating system including service pack level on tms02 is exactly the same as on tms01.
2. Check that the servers are both configured with the same time zone; failure to do this will mean that the start and end times of scheduled conferences are incorrect in the case of a switchover.
3. Run the Cisco TMS installer on tms02:
   a. Choose the *Custom* installation mode and enter the IP address of the external SQL server when prompted.
   b. Install to the same directory as on tms01 and use the same log directory as on tms01. This is important because the log directory path is stored as an Environment Variable in Windows and not in the SQL database.
   c. If HTTPS was enabled during installation on tms01, use the same certificate used on tms01.
4. After the server has rebooted, log in to the Cisco TMS web application to verify that it works correctly.
5. On tms02 go to **Administrative Tools > Configuration > Network Settings > Advanced Network Settings for Systems on Internal LAN**. Make sure the IP address is tms01 (10.0.0.10) and the host name is tms.example.com as the installer could have changed these values.
6. Open the Services Management Console on tms02:
   - Stop all the Cisco TMS services - they all have names starting with TMS.
   - Stop the Internet Information Services (IIS) service called World Wide Web Publishing Service.
   - Set the Startup Type of the IIS and TMS services to “Manual”.

Tms02 is now ready to act as a warm spare in the case of a failure on tms01.

Note that in **Administrative Tools > Server Maintenance > TMS Service Status** you will see the services for both servers. Click on **Clear List** to remove the stopped services on tms02 from the list.

Synchronizing local files

Some customizable files used by Cisco TMS are stored in the Windows server's local file system rather than in the tmsng database. The folders these files are stored in must be kept synchronized between the two nodes. See Appendix 2. Local files for synchronization [p.25] for a full list of the folders that must be synchronized.

Use your preferred method of synchronizing the folders. One way to do this is:

1. Create a shell script that uses xcopy/robocopy to copy files to the corresponding folders on tms02.
2. Use the Windows Task Scheduler on tms01 to run the script each hour.

If you swap the two servers in the event of a failure on the primary server, change the synchronization mechanism you set up for keeping the folders on tms01 and tms02 in synch so that it now synchronizes from tms02 to tms01.

Upgrading Cisco TMS

You must keep the Cisco TMS software versions on the primary and secondary servers consistent. After upgrading the primary server, you must upgrade the secondary server as soon as possible. If the primary server fails while the secondary server is on an older software version, you will not be able to swap the servers until you have upgraded the secondary server to the newer Cisco TMS software version.

1. Upgrade the primary server.
2. Upgrade the secondary server.
3. After the server has rebooted, log in to the Cisco TMS web application to verify that it works correctly.
4. In the Cisco TMS application go to **Administrative Tools > Configuration > Network Settings**.
5. Check that the following IP address(es) and host names are set to IP address: 10.0.0.10 and hostname: tms.example.com:
   - **Event Notification > SNMP Traphost IP Address**
   - **Advanced Network Settings for Systems on Internal LAN**: all fields
   - **Advanced Network Settings for Systems on Public Internet/Behind Firewall**
6. Stop the TMS services and set them to Manual again.

Recovery if the primary server fails

If the primary server: tms01 fails and becomes unusable, changing the secondary server: tms02 into an operational state will take no more than a few minutes.

1. Unplug tms01 from the network.
2. Change the IP address of tms02 to the old IP address of tms01, for example 10.0.0.10.
3. Verify that tms02 is reachable on its new IP address.
4. Open the TMS Tools application and go to **Configuration > Change DB Connect Settings**.
5. Click **OK** to verify that tms02 still has the correct password, as the password to the database might have changed since you initially set up tms02.
6. In the Services Management Console:
   a. Change the Startup Type of all the TMS services and the World Wide Web Publishing Service to *Automatic*.
   b. Start the services.

Tms02 is now the active Cisco TMS server. As you have instructed managed systems to use tms.example.com when communicating with Cisco TMS, no reconfiguration is needed on the managed systems themselves.

To verify that tms02 operates correctly:

1. Schedule a short conference two minutes into the future.
2. See that it launches and is torn down as expected.
3. Check that you can monitor it using the **Conference Control Center**.
4. Check that Cisco TMS generates a call detail record (CDR) for the conference.

To verify that Cisco TMS is communicating with systems:

1. Wait approximately 20 minutes for the TMS Database Scanner Service to complete a full run.
2. Go to **Systems > System Overview** in Cisco TMS.
3. Select all the systems in the tree to the left, and select **Network Settings > TMS To System Connectivity** in the tree to the right.
4. Click **View** and then check that no systems have their **Status** set to *NoResponse*.

Note that in **Administrative Tools > Server Maintenance > TMS Service Status** you will see the services for both servers. Click on **Clear List** to remove the stopped services on tms01 from the list.

Before connecting tms01 to your network:

1. Change its IP address to tms02's old value, for example 10.0.0.11.
2. Disable all the TMS services and IIS.

Once the problem with tms01 has been fixed, it will become the warm spare in case tms02 ever goes down.

Note: Do not add tms01 back to the network before changing its IP address to a new value. This will lead to IP address conflicts that will cause unpredictable behavior in Cisco TMS.

Database redundancy

Two of the SQL Server 2008 high-availability alternatives are appropriate for Cisco TMS: database mirroring and failover clustering.

Database mirroring

Database mirroring increases database availability by maintaining a hot spare database on another SQL Server instance. The primary SQL Server instance is referred to as the principal database. The principal database has a secure channel to a mirror database residing on another SQL Server instance, preferably located on another physical server.

In the database mirroring model, there are two types of transfer mechanisms, synchronous and asynchronous.

Synchronous transfer

If you are using synchronous mirroring, a transaction is not considered successfully completed until it is committed in both the principal and mirror databases. This guarantees that the two databases are always consistent. However, network speed and distance will affect database response times.

Asynchronous transfer

If performance is more important than data consistency, data transfers can be set up as asynchronous operations, but some data will then be lost in the case of a catastrophic failure in the principal database server.

Network requirements for asynchronous mirroring:

Minimum bandwidth = 10Mbps

Latency < 50ms

Jitter < 1ms

Packet drops < 1%

Changing the database connection string

The SQL Server database mirroring feature supports automatic failovers between the principal and mirror databases in the case of a failure on the principal database. However Cisco TMS does not,so the database configuration must be manually changed in Cisco TMS. If you are using the NLB redundancy model, this must be done on both Cisco TMS nodes:

1. Go to the TMS Tools application **> Configuration > Change Database Connection Settings**.
2. Change the **Database Server\Instance** to point to the mirror database and click **OK**.
3. Restart all the TMS services as well as IIS to complete the manual failover operation.

Placing the principal and mirror databases in two different physical locations while using synchronous mirroring is not supported by Cisco TMS, as transactions take too long to complete, causing slow responses in the application.

See the following Microsoft Developer Network (MSDN) article for documentation on how to set up a mirrored database in SQL Server 2008: SQL Server 2008 Database Mirroring Overview

Failover clustering

Database failover clustering is a server level redundancy model where two or more servers (called nodes) share resources. If one or more nodes fail, the remaining nodes in the cluster automatically pick up all services from the failing nodes. Only one node manages a particular SQL Server instance at any given time.

Each failover cluster instance has a logical resource group that includes:

- Network name
- IP address
- SQL Server Database Engine service

Clients use the network name and IP address as identifiers to connect to the instance, regardless of which node currently serves the instance.

During installation, point Cisco TMS to the clustered instance's network name or IP address.

No further reconfiguration is necessary on the Cisco TMS server .

No additional steps are required when upgrading Cisco TMS.

Requirements

Two or more servers running Windows Server 2008 Enterprise or Datacenter edition.

Each server must have:

- Two network interfaces
- Shared disk storage such as a storage area network (SAN)

The following white paper from Microsoft gives an in-depth description on planning, implementation, and administration of an SQL Server 2008 failover cluster: SQL Server 2008 Failover Clustering

Backups

We recommend scheduling a regular automated backup of the tmsng database.

Appendix 1. Example ACE configuration

After initial configuration of your Cisco ACE 4710 Appliance Control Engine load balancer, you can copy and paste this sample configuration to your ACE. All IP addresses, DNS names, usernames, and passwords must be amended to reflect your actual configuration prior to applying the settings to your load balancer.

```
!Assigning a recourse class for use as the default class (minimum required configuration)
resource-class TMS
limit-resource all minimum 10.00 maximum unlimited
limit-resource conc-connections minimum 10.00 maximum unlimited
limit-resource sticky minimum 10.00 maximum unlimited

!The software version used on the ACE: A5 1.2
boot system image:c4710ace-t1k9-mz.A5_1_2.bin

!Configuring the hostname of the loadbalancer
hostname loadbalancer

!Creating and assigning configuration to the Admin Context
context Admin

!Putting the Admin context into the resource class TMS
member TMS

!Creating access lists, here nothing is restricted
access-list ALL line 8 extended permit ip any any
access-list ALL line 9 extended permit icmp any any

!Creating Probes for health check of the TMS (change username/password)
probe https BOOKING-PROBE-TMS
description Checking to see if the booking module is running. running against port 443
port 443
interval 10
passdetect interval 10
ssl version all
credentials tms-service my_password
request method get url /tms/booking
expect status 200 400
probe https CITIES-PROBE-TCP-443
port 443
interval 10
passdetect interval 45
receive 20
ssl version all
expect status 200 400
append-port-hosttag
open 20
probe http PROBE-HTTP-80
port 80
interval 10
passdetect interval 45
receive 2
request method get url /tms
expect status 200 499
open 2

!This probe logs into TMS on HTTPS for verification (change username/password)
probe https TMS-Monitoring-443
description Monitor the TMS application
```

```
port 443
ssl version all
credentials tms-service my_password
request method get url /tms
expect status 200 400

!This probe logs into TMS on HTTP for verification (change username/password)
probe http TMS-Monitoring-80
credentials tms-service my_password
request method get url /tms
expect status 200 400
probe https TMS-WEBSERVICES-443
description Check if the booking services are running on 443
port 443
interval 10
ssl version all
credentials tms-service my_password
request method get url /TMS/external/booking/bookingservice.asmx
expect status 200 400

!Configuring the real servers
rserver host TMS01
description ***TMS01.EXAMPLE.COM***
ip address 10.0.200.50
inservice
rserver host TMS02
description ***TMS02.EXAMPLE.COM***
ip address 10.0.200.60
inservice

!Creating server farms
serverfarm host SFARM-TMS-WEB-161
description ** TMS-WEB-161 VIP **
probe PROBE-HTTP-80
rserver TMS01
inservice
rserver TMS02
inservice
serverfarm host SFARM-TMS-WEB-162
description ** TMS-WEB-162 VIP **
probe PROBE-HTTP-80
rserver TMS01
inservice
rserver TMS02
inservice
serverfarm host SFARM-TMS-WEB-443
description ** TMS-WEB-443 VIP **
probe BOOKING-PROBE-TMS
probe TMS-Monitoring-443
probe TMS-WEBSERVICES-443
rserver TMS01 443
inservice
rserver TMS02 443
inservice
serverfarm host SFARM-TMS-WEB-80
description ** TMS-WEB-80 VIP **
probe PROBE-HTTP-80
rserver TMS01 80
```

```
inservice
rserver TMS02 80
inservice

!Adding sticky sessions to all server farms
sticky ip-netmask 255.255.255.255 address source L7-CLASS-TMS-WEB-161-STICKY
timeout 10
serverfarm SFARM-TMS-WEB-161
sticky ip-netmask 255.255.255.255 address source L7-CLASS-TMS-WEB-162-STICKY
timeout 10
serverfarm SFARM-TMS-WEB-162
sticky ip-netmask 255.255.255.255 address source L7-CLASS-TMS-WEB-443-STICKY
timeout 10
serverfarm SFARM-TMS-WEB-443
sticky ip-netmask 255.255.255.255 address source L7-CLASS-TMS-WEB-80-STICKY
timeout 10

!Adding the virtual IP address to the virtual servers
serverfarm SFARM-TMS-WEB-80
class-map match-all L4-CLASS-TMS-WEB-161
match virtual-address 10.0.200.40 tcp eq 161
class-map match-all L4-CLASS-TMS-WEB-162
match virtual-address 10.0.200.40 tcp eq 162
class-map match-all L4-CLASS-TMS-WEB-443
match virtual-address 10.0.200.40 tcp eq https
class-map match-all L4-CLASS-TMS-WEB-80
match virtual-address 10.0.200.40 tcp eq www
class-map type http loadbalance match-any default-compression-exclusion-mime-type
description DM generated classmap for default LB compression exclusion mime types.
match http url .*gif
match http url .*css
match http url .*js
match http url .*class
match http url .*jar
match http url .*cab
match http url .*txt
match http url .*ps
match http url .*vbs
match http url .*xsl
match http url .*xml
match http url .*pdf
match http url .*swf
match http url .*jpg
match http url .*jpeg
match http url .*jpe
match http url .*png

!Making sure we can access the ACE remotely
class-map type management match-any remote_access
match protocol xml-https any
match protocol icmp any
match protocol telnet any
match protocol ssh any
match protocol http any
match protocol https any
match protocol snmp any
policy-map type management first-match remote_mgmt_allow_policy
class remote_access
```

```
permit
class class-default
permit

!Setting load balancing properties
policy-map type loadbalance first-match L4-CLASS-TMS-WEB-161-STICKY
class class-default
sticky-serverfarm L7-CLASS-TMS-WEB-161-STICKY
policy-map type loadbalance first-match L4-CLASS-TMS-WEB-162-STICKY
class class-default
sticky-serverfarm L7-CLASS-TMS-WEB-162-STICKY
policy-map type loadbalance first-match L4-CLASS-TMS-WEB-443-STICKY
class class-default
sticky-serverfarm L7-CLASS-TMS-WEB-443-STICKY
policy-map type loadbalance first-match L4-CLASS-TMS-WEB-80-STICKY
class class-default
sticky-serverfarm L7-CLASS-TMS-WEB-80-STICKY

!Setting virtual server properties
policy-map multi-match L4-POLICY-TMS-WEB
class L4-CLASS-TMS-WEB-162
loadbalance vip inservice
loadbalance policy L4-CLASS-TMS-WEB-162-STICKY
loadbalance vip icmp-reply
class L4-CLASS-TMS-WEB-161
loadbalance vip inservice
loadbalance policy L4-CLASS-TMS-WEB-161-STICKY
loadbalance vip icmp-reply
class L4-CLASS-TMS-WEB-80
loadbalance vip inservice
loadbalance policy L4-CLASS-TMS-WEB-80-STICKY
loadbalance vip icmp-reply
class L4-CLASS-TMS-WEB-443
loadbalance vip inservice
loadbalance policy L4-CLASS-TMS-WEB-443-STICKY

!Configuring virtual interface VLAN
interface vlan 200
description client
no ipv6 normalization
no ipv6 icmp-guard
ip address 10.0.200.24 255.255.255.0
no normalization
no icmp-guard
access-group input ALL
access-group output ALL
service-policy input remote_mgmt_allow_policy
service-policy input L4-POLICY-TMS-WEB
no shutdown

!END
```

Appendix 2. Local files for synchronization

During installation of Cisco TMS, customizable files are added which must be synchronized between the two servers when using a redundant deployment.

The files include software and images which can be uploaded to Cisco TMS, and images created by Cisco TMS.

In a default installation the files are located here:

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\CiscoSettings

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\CompanyLogo

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\ExternalSourceFiles

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\Image

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\Language

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logo

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\Map

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\MGCSettings

C:\Program Files\TANDBERG\TMS\wwwTMS\Public\Data\Software

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\Sound

Bibliography

All documentation for the latest version of Cisco TMS can be found at http://www.cisco.com/en/US/products/ps11338/tsd_products_support_series_home.html.

Title	Reference	Link
Cisco TelePresence Management Suite Installation and Getting Started Guide 13.2	D14389	http://cisco.com
Cisco TelePresence Management Suite Release Notes 13.2	D14952	http://cisco.com
Cisco TelePresence Management Suite Provisioning Extension Deployment Guide	D14941	http://cisco.com
SQL Server 2008 Database Mirroring Overview		http://msdn.microsoft.com
SQL Server 2008 Failover Clustering		http://download.microsoft.com