Cisco TelePresence Conductor Cluster Creation and Maintenance

Deployment Guide

XC1.2

D14828.03

May 2012

Contents

Introduction 3

Prerequisites 3
Network properties 3
TelePresence Conductor peer properties 3

Creating an initial cluster peer 4

Adding a peer to a cluster 5

Step 1: Configuring the cluster to accept the new peer 5
Step 2: Configuring the new peer to join the cluster 5
Step 3: Configuring the VCS to use the new cluster peer 5

Removing a peer from an existing cluster 7

Step 1: Removing the cluster peer from the VCS 7
Step 2: On the peer to be removed from the cluster 7
Step 3: On the other peers in the cluster 7

Maintenance routine 8

System backup 8

Appendix 1: Upgrading a cluster of TelePresence Conductors from XC1.1 to XC1.2 9

Step 1: Reconfiguring the policy server link on the VCS 9
Step 2: Removing the peers from the cluster 9
Step 3: Upgrading the peers that have been removed from the cluster 9
Step 4: Clustering the upgraded peer(s) 9
Step 5: Configuring the VCS(s) to point at the upgraded TelePresence Conductor peer(s) 10
Step 6: Upgrading the remaining cluster peer 10
Step 7: Adding the remaining cluster peer back into the cluster 10

Appendix 2: Clustered TelePresence Conductors and TMS 11

Legal notices 12

Intellectual property rights 12
Copyright notice 12

Introduction

Clusters of Cisco TelePresence Conductors are used to provide redundancy in the rare case of the failure of a TelePresence Conductor (for example, due to a network or power outage). Each TelePresence Conductor is a peer of the other TelePresence Conductors in the cluster. Configuration and conference status data is shared between all peers in the cluster. When the Cisco Video Communication Server (VCS) detects a TelePresence Conductor has failed the VCS automatically contacts a different TelePresence Conductor, which responds exactly as the failed one would. From an end users perspective this process is transparent and offers virtually no interruption in service.

This document will provide details on how to successfully:

- Create an initial cluster peer.
- Add a peer to the cluster.
- Remove a peer from the cluster.

Prerequisites

Network properties

- The resiliency that clustering introduces relies on the rapid sharing of information across cluster peers. As a result it is recommended that all the cluster peers communicate across a low latency connection.

- All cluster peers must be reachable using HTTPS from the VCSs they are going to receive conferencing requests from. Conference bridges in use by TelePresence Conductor must be reachable over HTTPS and/or HTTP on a per conference bridge basis.

- The following ports must be open between the TelePresence Conductor peers:

Service	Port	Protocol
IPSEC key exchange	500	UDP
EPMD	4369	UDP
Cluster replication	4371-4380	UDP & TCP

TelePresence Conductor peer properties

All cluster peers must be configured to use either the same NTP servers (**System > NTP**) or NTP servers which are very closely synchronized to provide conferencing services.

Creating an initial cluster peer

Note: For details on installing a TelePresence Conductor onto a network please refer to the *Cisco TelePresence Conductor Getting Started Guide* (D14829). This guide takes you through basic network configuration so your TelePresence Conductor can be contacted over the network.

1. Decide which peer is to be the initial peer. **The configuration of this peer will be shared with all other peers as they are added to the cluster**.
2. Check that no other TelePresence Conductor (anywhere) has this TelePresence Conductor's IP address in their clustering peers list.
3. Log into this peer as an administrator.
4. On the web interface of this TelePresence Conductor review the configuration to ensure that the TelePresence Conductor has:
   - a valid and working NTP server configured (**System > Time**; in the **Status** section the **State** should be *Synchronised*).
   - at least one valid DNS server configured **System > DNS**.
   - the correct **Domain name** and **System host name** configured.

     Note: <System host name>.<domain name> = FQDN of this TelePresence Conductor.

   - no peers configured (**System > Clustering** – all **Peer x IP address** fields on this page should be blank. If not, delete any entries and click **Save**)
   - no **Cluster pre-shared key** configured (**System > Clustering**)
5. On this peer, go to the **Clustering** page (**System > Clustering**)
6. Enter the following values in the relevant fields:

Field	Values
Cluster pre-shared key	Enter a password (this will be the same for all peers).
Peer 1 IP address	Enter the IP address of this Conductor peer (the initial peer in the cluster, from which configuration should be replicated).
Peer 2 IP address	Leave blank at this stage.
Peer 3 IP address	Leave blank at this stage.

7. Save this configuration.
8. Restart this peer (**Maintenance > Restart**, then click **Restart system**).

Adding a peer to a cluster

Step 1: Configuring the cluster to accept the new peer

On each existing cluster peer (i.e. the initial peer and any other peer that has already been added to the cluster):

1. Log in to this peer as a user with administrator privileges and go to the **Clustering** page (**System > Clustering**).
2. In the next empty **Peer IP address** field, enter the new peer's IP address.
3. **Save** this configuration.

Step 2: Configuring the new peer to join the cluster

Note: For details on installing a TelePresence Conductor onto a network please refer to the *Cisco TelePresence Conductor Getting Started Guide (D14829).* This guide takes you through basic network configuration so your TelePresence Conductor can be contacted over the network.

1. On the web interface of this TelePresence Conductor review the configuration to ensure that the TelePresence Conductor has:
   - a valid and working NTP server configured (**System > Time**; in the **Status** section the **State** should be *Synchronised*).
   - at least one valid DNS server configured **System > DNS**.
   - the correct **Domain name** and **System host name** configured.

     Note: <System host name>.<domain name> = FQDN of this TelePresence Conductor.

   - no peers configured (**System > Clustering** – all **Peer x IP address** fields on this page should be blank. If not, delete any entries and click **Save**)
   - no **Cluster pre-shared key** configured (**System > Clustering**)
2. On the new peer, go to the **Clustering** page (**System > Clustering**).
3. In the **Cluster pre-shared key** field, enter the same password as used for the initial peer.
4. In the **Peer 1 IP address** field, enter the initial peer's IP address.
5. In the remaining **Peer IP address** fields, enter the IP addresses of all peers in the cluster, including the new peer.
6. **Save** this configuration.
7. Restart this peer (**Maintenance > Restart**, then click **Restart system**).
8. Log in to the new peer.

Step 3: Configuring the VCS to use the new cluster peer

For every VCS that communicates with the TelePresence Conductor cluster directly:

1. Log into the VCS (or if the VCS is clustered the master VCS in the cluster) as a user with administrator privileges.
2. Go to the **Policy services** page (**VCS configuration > Dial plan > Policy services**)
3. Click on the policy service for the TelePresence Conductor.
4. In the uppermost blank **Server address** field enter the address of the Conductor peer you have added to the cluster.

5. Click **Save**.

Removing a peer from an existing cluster

Step 1: Removing the cluster peer from the VCS

1. Log into the VCS (or if the VCS is clustered the master VCS in the cluster) as a user with administrator privileges.
2. Go to the **Policy services** page (**VCS configuration > Dial plan > Policy services**)
3. Click on the policy service for the TelePresence Conductor.
4. Remove the address of the peer to be removed from the list of policy servers.
5. Click **Save**.

Step 2: On the peer to be removed from the cluster

Before removing a live peer from a cluster, you must place the peer in standalone mode so that it no longer communicates with other peers in the cluster. If the peer is out of service and can no longer be accessed, you do not need to place it in standalone mode. However, you must still follow the instructions to remove it from the cluster in the next section: **On the other peers in the cluster.**

To place a peer into standalone mode:

1. Log in to the peer to be removed from the cluster as a user with administrator privileges.
2. On the peer to be removed, go to the **Clustering** page (**System > Clustering**).
3. Delete the **Cluster pre-shared key**.
4. Delete all entries from the **Peer IP address** fields.
5. **Save** this configuration.
6. Restart the peer (**Maintenance > Restart**, then click **Restart system**).
7. Delete all entries from the conference bridge pool (**Conference configuration > Conference bridges > Conference bridge pools > All conference bridges)**.
8. Update the policy service on the VCS so that it does not include the removed peer. **System > Clustering**

Step 3: On the other peers in the cluster

After the peer to be removed has been placed in standalone mode (or if the peer is out of service and cannot be contacted), you must update all other peers in the cluster so they no longer consider the removed peer to be part of their cluster.

To do this, on each remaining peer in the cluster:

1. Go to the **Clustering** page (**System > Clustering**).
2. Delete the **Peer IP address** of the peer that has been removed from the cluster.
3. **Save** this configuration.
4. Repeat these steps for each remaining peer.

Maintenance routine

System backup

To create a system backup:

1. go to the **Backup and restore** page (**Maintenance > Backup and restore**).
2. Click **Create system backup file**.
3. Wait for the file download dialog to appear.
4. Click **Save** and save the backup file to an appropriate location.

Note: a system backup can only be restored to the peer upon which the backup was taken.

Appendix 1: Upgrading a cluster of TelePresence Conductors from XC1.1 to XC1.2

The process described here is essentially disbanding, upgrading and then reclustering a cluster of TelePresence Conductors. The basic process described intends to minimize downtime by only performing actions requiring downtime on those cluster peers that the VCS does not at that time send conference requests to.

Step 1: Reconfiguring the policy server link on the VCS

This step involves choosing one peer in the cluster to be the last to be upgraded. This cluster peer will service conference requests from the VCSs until the other peers have been upgraded and re-clustered.

For every VCS that communicates directly with TelePresence Conductor:

1. Go to the Cisco VCS web interface and log in as an admin user.
2. Go to the **Policy services** page (**VCS configuration > Dial plan > Policy services**).
3. Click "**View/Edit"** for the relevant policy server.
4. Remove the server addresses of the peers in the cluster you are going to upgrade initially leaving only one.
5. Click **Save.**

Step 2: Removing the peers from the cluster

The purpose of this step is to remove the peers from the cluster that are going to be upgraded first.

For each peer in the cluster that is not currently servicing conferencing requests complete the steps outlined in **steps 2** and **3** of **"Removing a peer from an existing cluster"**

Step 3: Upgrading the peers that have been removed from the cluster

For each peer that has been removed from the cluster:

1. Go to the Cisco Telepresence Conductor web interface and log in as an admin user.
2. Go to the **Upgrade page** page (**Maintenance > Upgrade**).
3. Click **Browse** and select the TelePresence Conductor XC1.2 software image.
4. Click **upgrade.**
5. Follow the onscreen prompts.

Step 4: Clustering the upgraded peer(s)

If you have only one upgraded peer (i.e you started with a cluster of two) follow the steps outlined in "**Creating an initial cluster peer".**

If you have two upgraded peers (i.e you started with a cluster of three) follow the steps outlined in "**Creating an initial cluster peer"** for the first peer then for the second peer perform the actions outlined in **Steps 1 and 2** of **"Adding a peer to a cluster"**

Step 5: Configuring the VCS(s) to point at the upgraded TelePresence Conductor peer(s)

For every VCS that communicates directly with TelePresence Conductor:

1. Go to the Cisco VCS web interface and log in as an admin user.
2. Go to the **Policy services** page (**VCS configuration > Dial plan > Policy services**).
3. Click "**View/Edit"** for the relevant policy server.
4. Remove the server addresses of the peer that has not been upgraded and insert the addresses of the peers that have been upgraded.
5. Click **Save.**

Step 6: Upgrading the remaining cluster peer

1. Go to the Cisco Telepresence Conductor web interface and log in as an admin user.
2. Go to the **Clustering page** page (**System > Clustering**).
3. Blank out all the clustering information.
4. Click **Save.**
5. Restart TelePresence Conductor.
6. Log in as an admin user.
7. Go to the **Upgrade page** page (**Maintenance > Upgrade**).
8. Click **Browse** and select the TelePresence Conductor XC1.2 software image.
9. Click **Upgrade.**

Step 7: Adding the remaining cluster peer back into the cluster

Follow the steps outlined in "**Adding a peer to a cluster**"

Appendix 2: Clustered TelePresence Conductors and TMS

As of TMS version 13.1.2 the solution for TMS integration is to add only one of the members of the TelePresence Conductor cluster to TMS. To do this follow the Instructions outlined in the TelePresence Conductor Deployment Guide 1.1.

Legal notices

Intellectual property rights

This Deployment Guide and the product to which it relates contain information that is proprietary to TANDBERG and its licensors. Information regarding the product is found below in the Copyright notice and Patent information sections.

TANDBERG® is a registered trademark belonging to Tandberg ASA. Other trademarks used in this document are the property of their respective holders. This Guide may be reproduced in its entirety, including all copyright and intellectual property notices, in limited quantities in connection with the use of this product. Except for the limited exception set forth in the previous sentence, no part of this Guide may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronically, mechanically, by photocopying, or otherwise, without the prior written permission of TANDBERG.

COPYRIGHT © TANDBERG

Copyright notice

The product that is covered by this Deployment Guide is protected under copyright, patent, and other intellectual property rights of various jurisdictions.

This product is Copyright © 2012, Tandberg Telecom UK Limited. All rights reserved.

TANDBERG is now part of Cisco. Tandberg Telecom UK Limited is a wholly owned subsidiary of Cisco Systems, Inc.

A list of the conditions of use can be found at:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/conductor/license_info/Cisco_Conductor_EULA.pdf

This product includes copyrighted software licensed from others. A list of the licenses and notices for open source software used in this product can be found at:
http://www.cisco.com/en/US/products/ps11775/products_licensing_information_listing.html

This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/).

This product includes software developed by the University of California, Berkeley and its contributors.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.