Replace X-series servers with Cisco Meeting Server appliance or Virtual Machine

Contents

Introduction

This document describes how to safely and reliably replace Acano X-Series servers with Cisco Meeting Server (CMS) Virtual Machines (VMs), CMS1000 or CMS2000 servers. The Acano X-Series servers support has been dropped from version 3.0 onwards. The latest software you can run on an X-Series is 2.9.5 which is only supported until March 1, 2022. After which, there will be no further maintenance releases or bug fixes. This means if you have an Acano X-Series server, you need to plan to replace them before that time.

Requirements

Cisco recommends that you have knowledge of these topics:

- CMS administration
- CMS upgrades
- Certificate creation and signing

Components Used

The information in this document is based on Cisco Meeting Server (VM or CMS1K, or CMS2K) and Acano X-Series servers.

The information in this document was created from the devices in a specific lab environment. If your network is live, ensure that you understand the potential impact of any command.

Background Information

When you replace your X-Series servers, you need to be aware of the call capacities of the various servers. Refer to the Cisco Meeting Server deployment guides, in Appendix C (https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-

configuration-guides-list.html) for sizing guidance.

X-Series sizes for reference:

- X1 - 25 HD (720p) calls
- X2 - 125 HD (720p) calls
- X3 - 250 HD (720p) calls

The process of the set up the replacement server can be found in the install documentation and is not covered below. Installation guides can be found here: https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-guides-list.html.

Replace X-series servers with CMS appliance or virtual machine

The supported method to replace the X-Series servers is to add the new device to the database cluster so it gets a copy of the database.

> **Caution**: Do not use a backup from a X-Series server to deploy your replacement.

Not every step below is required to complete the replacement. Cluster your new servers with the old servers so they get a copy of the database is the most important part.

Once you complete the migration process, all of your database information (inbound rules, outbound rules, cospaces, call ids, etc) is on the new servers as well.

> **Note**: Data entered in the graphical user interface (GUI) under **Configuration > General** and **Configuration > Active Directory** is NOT in the database. You must move your Lightweight Directory Access Protocol (LDAP) configuration from the GUI into the Application Programming Interface (API). If you are not prepared to do that yet, then copy all data from those two pages so they can be re-entered on the new servers. Be aware that the password for the LDAP username is required as well for LDAP because you cannot copy that information.

You will find a highlevel description of the work flow first, followed by the step by step instruction. It is highly recommended to follow the step by step instructions for the replacement procedure.

Highlevel description of work

Step 1. Create backup files from old Acano X-Series servers.

Step 2. Download the backup file and logbundle.tar.gz file from the old servers in case info is needed to configure new server's Mainboard Management Processor (MMP).

Step 3. On your old X-Series server, log into MMP and get the output of each service/config and copy the info into a note file.

Step 4. Set up new server(s).

Step 5. Get licenses on the new server(s).

Step 6. Copy certificates from old servers to new servers.

Step 7. Enable MMP services on the new servers that were set up on the old server.
(Acano X-series can use a dedicated Admin interface for management. You need to manage the new server via A-D interface, but all services on the new server can be on the A interface.)

Step 8. Create the same user accounts on the new servers that were used on the old servers.

Step 9. Copy the database to the new servers.

Step 10. Remove X-Series from the database cluster.

Step 11. Shut down the X-Series server that the new server replaces.

Step 12. Change the IP on the new device to match old X-Series interface A IP that is being replaced. If you use multiple interfaces on the X-Series, you must use them on the new servers also as this eliminates the need to change any DNS records.

Step 13. Join the server back to the database cluster (only if the original deployment was not a single combined server).

Step 14. Adjust the loadlimits accordingly on the new servers in the API - api/v1/system/configuration/cluster.

Step 15. Test the deployment to ensure it still works.

Step by step detailed instructions

Step 1. Create a backup using MMP command **backup snapshot <server_specific_filename>**.

Step 2. Download the backup file and a logbundle.tar.gz (https://video.cisco.com/video/5810051601001) file from each of the X-Series servers you want to replace.

Step 3. Run the following commands on the X-Series servers to get the configuration of the various services and put them in a note file. This provides an easy reference on how to reconfigure your new servers.

'webadmin', 'callbridge', 'webbridge', 'xmpp', 'turn', 'dns', 'ntp server list', 'tls sip', 'tls ldap', 'tls dtls', 'tls webadmin', 'database cluster status', 'user list', 'ipv4 a', 'ipv4 b', 'ipv4 c', 'ipv4 d', 'ipv4 admin', 'recorder', 'streamer', 'uploader', 'dscp', 'sipedge', 'h323_gateway', 'syslog', 'ldap'

> **Note**: H323_gateway, Sip Edge and XMPP are deprecated in CMS 3.0.
>
> If you use SIP Edge, you need to have a Cisco Expressway-C and E to route the traffic to and from the internet.
> If you use H323 gateway, you need to configure this using a Cisco Expressway server to perform the H.323 to SIP interworking.
> If you use XMPP, once you upgrade to CMS 3.x, you will need to make some configuration

changes. However, if you are about to replace the X-series and stay on 2.9.x for a while, and you need to use WebRTC, recorder or streamer, you need to reconfigure XMPP on your new server.

You can read more about the changes to be aware of before the upgrade to CMS 3.0 on this document.

Step 4. Set up the new servers. Ensure they have the same version of code as the X-Series servers. Give the servers non-used IPs to use for now (**ipv4 <interface> add <address>/<prefix length> <gateway>**), but when the work is completed, the IPs are changed to what was used on the X-Series. This is to avoid any change on DNS records and certificates. If you don't want to re-use the old IPs, you must update DNS and certificates accordingly.

Step 5. In the new server and the old X-Series server's MMP, run the command **iface a** to get the MAC address of the A interfaces. From the X-Series that is about to be replaced, download the cms.lic file and open a TAC Licensing case. Give the licensing agent the new server's interface A MAC address and the old server's MAC and tell them you want to replace the old server with a new one. Ask them to swap the licenses from the old MAC to the new MAC. A new license file is then provided, which you need to unzip, rename as cms.lic and upload to your new server.

Step 6. Copy the certificates, keys, and Certificate Authority (CA) files that are used on the old X-Series to the new server(s) using WinSCP or any other SFTP program.

Step 7. On the new server, enable the same services and settings in MMP that you currently have on your old X-Series. Refer to the info you gathered in Step 3, to ensure you make the same configurations as before.

Note: If you are going to upgrade to CMS 3.x immediately after the set up of these new servers, you do not need to configure the XMPP, Webbridge, SIP Edge, or H323_gateway components. These are no longer used in CMS 3.x.

Step 8. Create the same user accounts that were on the X-Series servers on the MMP using the command **user add <username> <role>** (as well as **user rule <rule name> <value>** if you have any rules set up). Other devices such as Cisco Meeting Management (CMM), TelePresence Management Suite (TMS), or Cisco Unified Communications Manager (CUCM) can be set up for features with these accounts, so you need to ensure you set them up on the new servers.

Step 9. Get a copy of the database on to the new server(s).

9a. If the current deployment is a single combined server (no database cluster), you need to initialize a database cluster on it. From CMS version 2.7 onwards, a database cluster requires certificates. Therefore a built in Certificate Authority has been introduced into CMS from version 2.7 onwards that you can use to sign your database certificates:

1. On the single combined X-Series MMP, run **pki selfsigned dbca CN:<Company Name>** (ex. pki selfsigned dbca CN:tplab.local)

2. On the single combined X-Series MMP, create a certificate for database server with **pki csr dbserver CN:xseries.example.com subjectAltName:<newcms1fqdn>**

(You don't need to have DNS A records at this point for this.)

3. On the single combined X-Series MMP, create a certificate for database client with **pki csr dbclient CN:postgres**

4. On the single combined X-Series MMP, use dbca (from Step 1) to sign the dbserver (from Step 2) certificate **pki sign dbserver dbca**

5. On the single combined X-Series MMP, use dbca (from Step 1) to sign the dbclient (from Step 3) certificate **pki sign dbclient dbca**

6. Copy the dbserver.crt, dbserver.key, dbclient.crt and dbclient.key files to all of the server(s) that will be joined to the database (nodes that make up the database cluster) from the X-Series to the new server(s)

7. Copy the dbca.crt file to all of the server(s) from the X-Series

8. On the single combined X-Series MMP, run **database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt** (dbca.crt as the root CA certificate)

9. On the single combined X-Series MMP, run **database cluster localnode a**

10. On the single combined X-Series MMP, run **database cluster initialize**

11. On the single combined X-Series MMP, run **database cluster status**. You must see:
Nodes: <XseriesIP> (me) : Connected Primary

12. On the new server(s) that you will join to the database cluster, from MMP run **database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt**

13. On the new server(s) that you will join (co-located with a database), from MMP:

a. run **database cluster localnode a**

b. run **database cluster join <primary node IP**>

At this point, the new server(s) has/have a copy of the database. Run **database cluster status** in MMP on the new server to ensure they show as in sync. If they are, you are done with Step 9 and can continue to Step 10. However, if they are not in sync, you must review your database cluster configurations and ensure there is nothing in the network that would block communication over TCP 5432 between the servers.

9b. If the current deployment is already a database cluster, you want to replace the X-Series servers one at a time. On the X-Series, run in MMP **database cluster status** to verify if the server is joined to the database cluster or connected. If the server's IP is in the database cluster list, it is joined. If it is not, and the last command shown is 'database cluster connect', then the node is connected.

You want to add the new node back in as the same role (joined or connected), so take note of what the role of the X-Series server. If the X-Series is the database primary, reboot the server first so it becomes a replica.

1. On the X-Series that is about to be replaced, note the certificates used for server key/certificate, client key/certificate and CA certificate

2. On the X-Series that is about to be replaced, run **database cluster remove**

Step 10. If you replace a **single combined X-Series server**, continue here with Step 10. If it is a cluster, skip to Step 11.

At this point, the new server has a copy of the database. You can confirm this with a login into the new server's web interface and check the users and spaces configuration. After confirmation, now remove the new server from the database cluster and change the IP(s):

1. On the new server, run '**database cluster remove**'.

2. Shut down the X-Series server.

3. Change the IP(s) on the new server to the ones used on the X-Series server.

4. Reboot the new server.

5. If you stay on CMS 2.9.x version, test the new server to ensure all configurations work.

6. Log into the web admin page of the new server, and look at the spaces and users. You must see all spaces and users that were previously in the server when joined to the database earlier as it took a copy of that.

Step 11. If you replace a X-Series server that is part of a cluster, you can follow the next steps:

1. Shut down the X-Series server that we plan to decommision.

2. Change the IPs on the new server to what was used previously on the X-Series server's database localnode interface (typically a).

3. Copy the server key/certificate, client key/certificate and CA Certificate to the new server with a SFTP program.

4. On the new server, run the command: '**database cluster localnode a**'

5a. If the new node is to be joined to the database cluster, run the command '**database cluster certs <server.key> <server.crt> <client.key> <client.crt> <ca.crt>**'

5b. If the new node is to be connected (not co-located with a database) to the database cluster, run the command '**database cluster certs <client.key> <client.crt> <ca.crt>**'.

6a. If the new node needs to be joined (co-located with a database) run the command: '**database cluster join <primary node IP>**'

6b. If the new node needs to be connected (not co-located with a database) run the command:'**database cluster connect <primary node IP>'**

Repeat Step 9b and 11 for each X-series you need to decommission.

Step 12. At this point, the new CMS servers will have a copy of the database, or if connected, know how to reach the database nodes and they have the same IP addresses as before as well.

Step 13. Is Load balancing enabled on your deployment?

If you use the CMS call load balancing with the CallBridgeGroups on the API set up with Loadbalancing=True, you must change the load limit to match the recommended limits of the new servers in the environment. Go to **api/v1/system/configuraiton/cluster** and update the loadlimit accordingly:

System	Recommended loadlimit
CMS1000 M5v2	120000
CMS1000 M4 or M5v1	96000
CMS2000 M5v2	875000
CMS2000	700000
VM (Number of vCPU x 1250)	example: 70 vCPU x 1250 = 87500

Step 14. If you had an XMPP cluster before this work and you intend to stay on CMS 2.9.x for a while, you need to rebuild your XMPP cluster.

MMP commands	**Examples**
Configure on all XMPP Nodes	**Configure on all XMPP Nodes**
1. xmpp reset	1. xmpp reset
2. xmpp domain <domain name>	2. xmpp domain example.com
3. xmpp listen <interface whitelist>	3. xmpp listen a
4. xmpp certs <keyfile> <certificate file> <cert-bundle>	4. xmpp certs xmppcluster.key xmppcluster.cer root.
5. xmpp cluster trust <xmpp cert>	5. xmpp cluster trust xmppcluster.cer ***** Note 1**
Configuration of the 1st Node	**Configuration of the 1st Node**
6. xmpp enable	6 xmpp enable
7. xmpp callbridge add <callbridge name>	7. xmpp callbridge add cb1
8. xmpp callbridge add <callbridge name>	8. xmpp callbridge add cb2
9. xmpp callbridge add <callbridge name>	9. xmpp callbridge add cb3
10. xmpp callbridge add <callbridge name>	10. xmpp callbridge add cb4 ***** Note 2**
11. xmpp callbridge list	11. xmpp callbridge list <--- copy this output to note
12. xmpp disable	12. xmpp disable
13. xmpp cluster enable	13. xmpp cluster enable
14. xmpp cluster initialize	14. xmpp cluster initialize
15. xmpp enable	15. xmpp enable
16. xmpp cluster status	16. xmpp cluster status
Configuration of 2nd and 3rd Node	**Configuration of 2nd and 3rd Node**
17. xmpp enable	17. xmpp enable
18. xmpp callbridge add-secret <callbridge name>	18. xmpp callbridge add-secret cb1
19. enter callbridge secret:	19. Enter callbridge secret: <copy secret for cb1 fron notepad>
20. xmpp callbridge add-secret <callbridge name>	20. xmpp callbridge add-secret cb2
21. Enter callbridge secret:	21. Enter callbridge secret: <copy secret for cb2 fron notepad>
22. xmpp callbridge add-secret <callbridge name>	22. xmpp callbridge add-secret cb3
23. Enter callbridge secret:	23: Enter callbridge secret: <copy secret for cb3 fron notepad>
24. xmpp callbridge add-secret <callbridge name>	24. xmpp callbridge add-secret cb4 ***** Note 3**
25. Enter callbridge secret:	25. Enter callbridge secret: <copy secret for cb4 fron notepad>
26. xmpp disable	26. xmpp disable
27. xmpp cluster enable	27. xmpp cluster enable
28. xmpp enable	28. xmpp enable
29. xmpp cluster join <cluster>	29. xmpp cluster join <IP address or FQDN of Node
Configure XMPP settings in Web Admin	**Configure XMPP settings in Web Admin**

On each server with CallBridge service	On each server with CallBridge service
30. Enter this callbridges Unique Name configured above	30. Enter cb1 on callbridge1, etc
31. Enter the domain	31. Enter domain: example.com
32. Enter the secret from notepad	32. Enter secret from notepad for corresponding callbridge
33. Check webadmin status page for authentication	33. Check webadmin status page for authentication

Note 1: xmpp cluster trust in example is the XMPP certificate because the certificate contains all XMPP server FQDNs in the Subject Alternative Name (SAN) attribute, or is a wild card certificate. If each XMPP server has its own certificate, you need to combine them, and add them as the xmpp cluster trust.

Note 2: xmpp callbridge add cb4. Added this step as an example that you can have more callbridges than you have xmpp servers. This step is not necessary, but was added as an example.

Note 3: xmpp callbridge ad-secret cb4. Added this step to go along with Note 2. If you have 4 callbridges, you need to add all 4 to all nodes in the xmpp cluster.

If you stay on CMS 2.9.x version, you can begin the tests and validation now to ensure the new server(s) work(s) as expected.

Verify

After the migration to the new server(s), check that all of your users and spaces are visible, and that your SIP calls still work. If you stay on CMS 2.9.x version, confirm that XMPP works still (WebRTC users can still join/sign in, recorder can connect, etc). Check any servers that are in communication with CMS to ensure they are still functional (Cisco Meeting Manager (CMM), Cisco Unified Communications Manager (CUCM), TelePresence Management Suite (TMS), Expressway). It is also a good idea to run 'syslog follow' in the MMP to see if there are any errors that need to be addressed.

Troubleshoot

If you run into any issues, you can revert back to your X-Series servers, or contact Cisco TAC for support.