Remplacer les serveurs de la gamme X par l'appliance Cisco Meeting Server ou la machine virtuelle

Contenu

Introduction

Ce document décrit comment remplacer en toute sécurité et de manière fiable les serveurs Acano X par des serveurs Cisco Meeting Server (CMS) Virtual Machines (VM), CMS1000 ou CMS2000. La prise en charge des serveurs de la gamme Acano X a été supprimée à partir de la version 3.0. Le dernier logiciel que vous pouvez exécuter sur une série X est 2.9.5, qui n'est pris en charge que jusqu'au 1er mars 2022. Après quoi, il n'y aura plus de versions de maintenance ou de corrections de bogues. Cela signifie que si vous avez un serveur Acano série X, vous devez prévoir de les remplacer avant cette date.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration CMS
- Mises à niveau CMS
- Création et signature de certificats

Components Used

Les informations de ce document sont basées sur les serveurs Cisco Meeting Server (VM, CMS1K ou CMS2K) et Acano X.

The information in this document was created from the devices in a specific lab environment. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Lorsque vous remplacez vos serveurs de la gamme X, vous devez connaître les capacités d'appel des différents serveurs. Reportez-vous aux guides de déploiement de Cisco Meeting Server, à l'annexe C (https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html) pour obtenir des conseils sur le dimensionnement.

Tailles de série X pour référence :

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

Le processus de configuration du serveur de remplacement se trouve dans la documentation d'installation et n'est pas couvert ci-dessous. Les guides d'installation sont disponibles ici : https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-guides-list.html.

Remplacer les serveurs de la série X par une appliance CMS ou une machine virtuelle

La méthode prise en charge pour remplacer les serveurs de la série X consiste à ajouter le nouveau périphérique au cluster de base de données afin qu'il obtienne une copie de la base de données.

> **Attention** : N'utilisez pas de sauvegarde à partir d'un serveur série X pour déployer votre remplacement.

Toutes les étapes ci-dessous ne sont pas nécessaires pour effectuer le remplacement. Regroupez vos nouveaux serveurs avec les anciens serveurs afin qu'ils obtiennent une copie de la base de données est la partie la plus importante.

Une fois le processus de migration terminé, toutes les informations de votre base de données (règles entrantes, règles sortantes, espaces communs, ID d'appel, etc.) se trouvent également sur les nouveaux serveurs.

> **Note**: Les données entrées dans l'interface utilisateur graphique (GUI) sous **Configuration > General** and **Configuration > Active Directory** ne figurent PAS dans la base de données. Vous devez déplacer votre configuration LDAP (Lightweight Directory Access Protocol) de l'interface utilisateur graphique vers l'API (Application Programming Interface). Si vous n'êtes pas encore prêt à le faire, copiez toutes les données de ces deux pages afin qu'elles puissent être entrées à nouveau sur les nouveaux serveurs. Sachez que le mot de passe du nom d'utilisateur LDAP est également requis pour LDAP car vous ne pouvez pas copier ces informations.

Vous trouverez d'abord une description détaillée du flux de travail, suivie de l'instruction pas à pas. Il est fortement recommandé de suivre les instructions étape par étape pour la procédure de remplacement.

Description du travail de haut niveau

Étape 1. Créez des fichiers de sauvegarde à partir d'anciens serveurs de la gamme Acano X.

Étape 2. Téléchargez le fichier de sauvegarde et le fichier logbundle.tar.gz à partir des anciens serveurs au cas où des informations seraient nécessaires pour configurer le nouveau serveur MMP (Mainboard Management Processor).

Étape 3. Sur votre ancien serveur X-Series, connectez-vous à MMP et obtenez le résultat de chaque service/config et copiez les informations dans un fichier de notes.

Étape 4. Configurer de nouveaux serveurs.

Étape 5. Obtenez des licences sur les nouveaux serveurs.

Étape 6. Copier les certificats des anciens serveurs vers les nouveaux serveurs.

Étape 7. Activez les services MMP sur les nouveaux serveurs configurés sur l'ancien serveur. (La gamme Acano X peut utiliser une interface Admin dédiée pour la gestion. Vous devez gérer le nouveau serveur via l'interface A-D, mais tous les services du nouveau serveur peuvent se trouver sur l'interface A.)

Étape 8. Créez les mêmes comptes utilisateur sur les nouveaux serveurs qui ont été utilisés sur les anciens serveurs.

Étape 9. Copiez la base de données sur les nouveaux serveurs.

Étape 10. Supprimez la série X du cluster de base de données.

Étape 11. Arrêtez le serveur X-Series que le nouveau serveur remplace.

Étape 12. Modifiez l'adresse IP sur le nouveau périphérique pour qu'elle corresponde à l'ancienne adresse IP de la série X qui est remplacée. Si vous utilisez plusieurs interfaces sur la série X, vous devez également les utiliser sur les nouveaux serveurs, car cela évite de devoir modifier les enregistrements DNS.

Étape 13. Rejoindre le serveur au cluster de base de données (uniquement si le déploiement initial n'était pas un seul serveur combiné).

Étape 14. Ajustez les limites de charge en conséquence sur les nouveaux serveurs de l'API - api/v1/system/configuration/cluster.

Étape 15. Testez le déploiement pour vous assurer qu'il fonctionne toujours.

Instructions détaillées étape par étape

Étape 1. Créez une sauvegarde à l'aide de la commande MMP **backup snapshot <nom_fichier_spécifique_serveur>**.

Étape 2. Téléchargez le fichier de sauvegarde et un fichier logbundle.tar.gz (https://video.cisco.com/video/5810051601001) à partir de chacun des serveurs de la série X que vous voulez remplacer.

Étape 3. Exécutez les commandes suivantes sur les serveurs de la gamme X pour obtenir la

configuration des différents services et les placer dans un fichier de notes. Cela fournit une référence facile sur la reconfiguration de vos nouveaux serveurs.

'webadmin', 'callbridge', 'webbridge', 'xmpp', 'tour', 'dns', 'liste de serveurs ntp', 'tls sip', 'tls ldap', 'tls dtls', 'tls webadmin', 'état du cluster de base de données', 'liste d'utilisateurs', 'ipv4 a', 'ipv4 b', 'ipv4 c' , 'ipv4 d', 'ipv4 admin', 'enregistreur', 'streaming', 'uploader', 'dscp', 'sipedge', 'h323_gateway', 'syslog', 'ldap'

> **Note**: H323_gateway, Sip Edge et XMPP sont déconseillés dans CMS 3.0.
>
> Si vous utilisez SIP Edge, vous devez disposer d'un Cisco Expressway-C et E pour acheminer le trafic vers et depuis Internet.
> Si vous utilisez une passerelle H323, vous devez configurer cette fonctionnalité à l'aide d'un serveur Cisco Expressway pour effectuer l'interconnexion H.323 vers SIP.
> Si vous utilisez XMPP, une fois la mise à niveau vers CMS 3.x effectuée, vous devrez apporter des modifications à la configuration. Cependant, si vous êtes sur le point de remplacer la série X et que vous restez sur 2.9.x pendant un certain temps et que vous devez utiliser WebRTC, un enregistreur ou un lecteur, vous devez reconfigurer XMPP sur votre nouveau serveur.
>
> Vous pouvez en savoir plus sur les modifications à prendre en compte avant la mise à niveau vers CMS 3.0 sur ce document.

Étape 4. Configurez les nouveaux serveurs. Assurez-vous qu'ils ont la même version de code que les serveurs de la série X. Donnez aux serveurs les adresses IP non utilisées à utiliser pour l'instant (**ipv4 <interface> add <address>/<prefix length> <gateway>**), mais une fois le travail terminé, les adresses IP sont remplacées par celles utilisées sur la série X. Ceci afin d'éviter toute modification des enregistrements et certificats DNS. Si vous ne voulez pas réutiliser les anciennes adresses IP, vous devez mettre à jour le DNS et les certificats en conséquence.

Étape 5. Dans le nouveau serveur et l'ancien MMP du serveur X, exécutez la commande **face a** pour obtenir l'adresse MAC des interfaces A. À partir de la série X sur le point d'être remplacée, téléchargez le fichier cms.lic et ouvrez un dossier de licence TAC. Donnez à l'agent de licence l'adresse MAC de l'interface A du nouveau serveur et l'adresse MAC de l'ancien serveur et indiquez-leur que vous voulez remplacer l'ancien serveur par un nouveau. Demandez-leur d'échanger les licences de l'ancien MAC vers le nouveau MAC. Un nouveau fichier de licence est ensuite fourni, que vous devez décompresser, renommer cms.lic et télécharger sur votre nouveau serveur.

Étape 6. Copiez les certificats, clés et fichiers d'autorité de certification (CA) utilisés sur l'ancienne série X sur le ou les nouveaux serveurs à l'aide de WinSCP ou de tout autre programme SFTP.

Étape 7. Sur le nouveau serveur, activez les mêmes services et paramètres dans MMP que ceux de votre ancienne série X. Reportez-vous aux informations que vous avez recueillies à l'étape 3 pour vous assurer que vous effectuez les mêmes configurations qu'auparavant.

> **Note**: Si vous effectuez une mise à niveau vers CMS 3.x immédiatement après la configuration de ces nouveaux serveurs, vous n'avez pas besoin de configurer les composants XMPP, Webbridge, SIP Edge ou H323_gateway. Ils ne sont plus utilisés dans CMS 3.x.

Étape 8. Créez les mêmes comptes d'utilisateur que ceux qui se trouvaient sur les serveurs de la série X du MMP à l'aide de la commande **user add <nom d'utilisateur> <rôle>** (ainsi que de la **règle d'utilisateur <nom de règle> <valeur>** si vous avez des règles configurées). D'autres périphériques, tels que Cisco Meeting Management (CMM), TelePresence Management Suite (TMS) ou Cisco Unified Communications Manager (CUCM), peuvent être configurés pour les fonctionnalités de ces comptes. Vous devez donc vous assurer de les configurer sur les nouveaux serveurs.

Étape 9. Obtenez une copie de la base de données sur les nouveaux serveurs.

9 bis. Si le déploiement actuel est un serveur combiné unique (pas de cluster de base de données), vous devez initialiser un cluster de base de données sur celui-ci. À partir de la version 2.7 de CMS, un cluster de base de données nécessite des certificats. Par conséquent, une autorité de certification intégrée a été introduite dans CMS à partir de la version 2.7 que vous pouvez utiliser pour signer vos certificats de base de données :

1. Sur le MMP unique combiné série X, exécutez **pki autosigné dbca CN:<Company Name>** (ex. pki selfsigned dbca CN : tplab.local)

2. Sur le MMP unique combiné série X, créez un certificat pour le serveur de base de données avec **pki csr dbserver CN : xseries.example.com subjectAltName :<newcms1fqdn>**

(Vous n'avez pas besoin d'enregistrements DNS A pour le moment.)

3. Sur le MMP unique combiné série X, créez un certificat pour le client de base de données avec **pki csr dbclient CN : postgres**

4. Sur le MMP unique combiné série X, utilisez dbca (à partir de l'étape 1) pour signer le **symbole pki du** certificat dbserver (à partir de l'étape 2) **dbserver dbca**

5. Sur le MMP unique combiné série X, utilisez dbca (à partir de l'étape 1) pour signer le **symbole pki du** certificat dbclient (à partir de l'étape 3) **dbclient dbca**

6. Copiez les fichiers dbserver.crt, dbserver.key, dbclient.crt et dbclient.key sur tous les serveurs qui seront joints à la base de données (noeuds constituant le cluster de base de données) à partir de la série X vers le ou les nouveaux serveurs

7. Copiez le fichier dbca.crt sur tous les serveurs de la série X

8. Sur le MMP unique combiné de la série X, exécutez **le cluster de base de données certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt** (dbca.crt en tant que certificat d'autorité de certification racine)

9. Sur le MMP unique combiné série X, exécutez le **noeud local du cluster de base de données a**

10. Sur le MMP unique combiné série X, exécutez **l'initialisation du cluster de base de données**

11. Sur le MMP unique combiné série X, exécutez l'**état du cluster de base de données**. Vous devez voir :
Noeuds : <XseriesIP> (moi) : Principal connecté

12. Sur le ou les nouveaux serveurs que vous allez joindre au cluster de base de données, à partir du **cluster de base de données** MMP exécuté **certs dbserver.key dbserver.crt dbclient.key**

dbclient.crt dbca.crt

13. Sur le ou les nouveaux serveurs auxquels vous allez vous connecter (colocalisé avec une base de données), à partir de MMP :

a. exécuter **localnode a du cluster de base de données**

b. exécuter **la jointure de cluster de base de données <noeud principal IP>**

Àce stade, le ou les nouveaux serveurs ont/ont une copie de la base de données. Exécutez **l'état du cluster de base de données** dans MMP sur le nouveau serveur pour vous assurer qu'ils s'affichent comme synchronisés. Si c'est le cas, vous avez terminé l'étape 9 et pouvez passer à l'étape 10. Cependant, s'ils ne sont pas synchronisés, vous devez vérifier les configurations de votre cluster de base de données et vous assurer qu'il n'y a rien dans le réseau qui bloquerait la communication sur TCP 5432 entre les serveurs.

9 ter. Si le déploiement actuel est déjà un cluster de base de données, vous voulez remplacer les serveurs de la série X un par un. Sur la série X, exécutez l'**état du cluster de base de données** MMP pour vérifier si le serveur est joint au cluster de base de données ou connecté. Si l'adresse IP du serveur figure dans la liste des clusters de base de données, elle est jointe. Si ce n'est pas le cas, et que la dernière commande affichée est 'database cluster connect', le noeud est connecté.

Vous souhaitez réajouter le nouveau noeud en tant que même rôle (joint ou connecté), alors prenez note du rôle du serveur de la série X. Si la série X est la base de données principale, redémarrez d'abord le serveur pour qu'il devienne un réplica.

1. Sur la série X sur le point d'être remplacée, notez les certificats utilisés pour la clé/le certificat du serveur, la clé/le certificat du client et le certificat de l'autorité de certification

2. Sur la série X qui est sur le point d'être remplacée, exécutez **la suppression du cluster de base de données**

Étape 10. Si vous remplacez un **seul serveur combiné de la série X**, passez à l'étape 10. S'il s'agit d'un cluster, passez à l'étape 11.

Àce stade, le nouveau serveur a une copie de la base de données. Vous pouvez le confirmer en vous connectant à l'interface Web du nouveau serveur et vérifier la configuration des utilisateurs et des espaces. Après confirmation, supprimez maintenant le nouveau serveur du cluster de base de données et modifiez les adresses IP :

1. Sur le nouveau serveur, exécutez '**suppression du cluster de base de données**'.

2. Arrêtez le serveur de la série X.

3. Remplacez les adresses IP du nouveau serveur par celles utilisées sur le serveur série X.

4. Redémarrez le nouveau serveur.

5. Si vous restez sur la version CMS 2.9.x, testez le nouveau serveur pour vous assurer que toutes les configurations fonctionnent.

6. Connectez-vous à la page d'administration Web du nouveau serveur et examinez les espaces

et les utilisateurs. Vous devez voir tous les espaces et utilisateurs qui se trouvaient précédemment dans le serveur lors de leur connexion à la base de données plus tôt, car il en a pris une copie.

Étape 11. Si vous remplacez un serveur de la gamme X faisant partie d'un cluster, vous pouvez suivre les étapes suivantes :

1. Arrêtez le serveur de la série X que nous prévoyons de décomposer.

2. Remplacez les adresses IP du nouveau serveur par celles qui étaient précédemment utilisées sur l'interface de noeud local de base de données du serveur de la série X (généralement a).

3. Copiez la clé/le certificat du serveur, la clé/le certificat du client et le certificat CA sur le nouveau serveur à l'aide d'un programme SFTP.

4. Sur le nouveau serveur, exécutez la commande suivante : '**cluster de base de données localnode a**'

5 bis. Si le nouveau noeud doit être joint au cluster de base de données, exécutez la commande '**database cluster certs <server.key> <server.crt> <client.key> <client.crt> <ca.crt>**'

5 ter. Si le nouveau noeud doit être connecté (non colocalisé avec une base de données) au cluster de base de données, exécutez la commande '**database cluster certs <client.key> <client.crt> <ca.crt>**'.

6 bis. Si le nouveau noeud doit être joint (colocalisé avec une base de données), exécutez la commande : '**jointure de cluster de base de données <noeud principal IP>**'

6 ter. Si le nouveau noeud doit être connecté (non colocalisé avec une base de données), exécutez la commande : **database cluster connect <adresse IP du noeud principal>'**

Répétez les étapes 9b et 11 pour chaque série X que vous devez déclasser.

Étape 12. À ce stade, les nouveaux serveurs CMS disposeront d'une copie de la base de données, ou, s'ils sont connectés, sauront comment atteindre les noeuds de base de données et ils auront les mêmes adresses IP qu'auparavant.

Étape 13. L'équilibrage de charge est-il activé sur votre déploiement ?

Si vous utilisez l'équilibrage de charge d'appels CMS avec CallBridgeGroups sur l'API configurée avec LoadBalayage=True, vous devez modifier la limite de charge pour qu'elle corresponde aux limites recommandées des nouveaux serveurs dans l'environnement. Accédez à **api/v1/system/configuration/cluster** et mettez à jour la limite de charge en conséquence :

système	Limite de charge recommandée
CMS1000 M5v2	120000
CMS1000 M4 ou M5v1	96000
CMS2000 M5v2	875000
CMS2000	700000
VM (nombre de vCPU x 1 250)	exemple : 70 vCPU x 1 250 = 87 500

Étape 14. Si vous aviez un cluster XMPP avant ce travail et que vous comptez rester sur CMS 2.9.x pendant un certain temps, vous devez reconstruire votre cluster XMPP.

Commandes MMP

Configurer sur tous les noeuds XMPP

1. xmpp reset
2. xmpp domain <nom de domaine>
3. xmpp hear <liste blanche d'interface>
4. xmpp certs <keyfile> <certificat file> <cert-bundle>
5. xmpp cluster trust <xmpp cert>

Configuration du 1er noeud

6. xmpp enable
7. xmpp callbridge add <nom du pont d'appel>
8. xmpp callbridge add <nom du pont d'appel>
9. xmpp callbridge add <nom du pont d'appel>
10. xmpp callbridge add <nom du pont d'appel>
11. xmpp callbridge list
12. xmpp disable
13. xmpp cluster enable
14. xmpp cluster initialize
15. xmpp enable
16. état du cluster xmpp

Configuration des 2e et 3e noeuds

17. xmpp enable
18. xmpp callbridge add-secret <nom du pont d'appel>
19. saisissez callbridge secret :
20. xmpp callbridge add-secret <nom du pont d'appel>
21. Entrez callbridge secret :
22. xmpp callbridge add-secret <nom du pont d'appel>
23. Entrez callbridge secret :
24. xmpp callbridge add-secret <nom du pont d'appel>
25. Entrez callbridge secret :
26. xmpp disable
27. xmpp cluster enable
28. xmpp enable
29. xmpp cluster join <cluster>

Configurer les paramètres XMPP dans Web Admin

Sur chaque serveur avec le service CallBridge

30. Entrez ce nom unique de ponts d'appel configuré ci-dessus
31. Entrez le domaine
32. Entrez le secret à partir du bloc-notes
33. Vérifier la page d'état de webadmin pour

Exemples

Configurer sur tous les noeuds XMPP

1. xmpp reset
2. xmpp domain example.com
3. xmpp Listen a
4. xmpp certs xmppcluster.key xmppcluster.cer root.cer
5. xmpp cluster trust xmppcluster.cer *** Note 1

Configuration du 1er noeud

6 xmpp enable
7. xmpp callbridge add cb1
8. xmpp callbridge add cb2
9. xmpp callbridge add cb3
10. xmpp callbridge add cb4 *** Note 2
11. xmpp callbridge list < : copiez ce résultat sur le bloc notes
12. xmpp disable
13. xmpp cluster enable
14. xmpp cluster initialize
15. xmpp enable
16. état du cluster xmpp

Configuration des 2e et 3e noeuds

17. xmpp enable
18. xmpp callbridge add-secret cb1
19. Entrez callbridge secret : <secret de copie pour cb1 partir du bloc-notes>
20. xmpp callbridge add-secret cb2
21. Entrez callbridge secret : <secret de copie pour cb2 partir du bloc-notes>
22. xmpp callbridge add-secret cb3
23: Entrez callbridge secret : <secret de copie pour cb3 partir du bloc-notes>
24. xmpp callbridge add-secret cb4 *** Note 3
25. Entrez callbridge secret : <secret de copie pour cb4 partir du bloc-notes>
26. xmpp disable
27. xmpp cluster enable
28. xmpp enable
29. xmpp cluster join <adresse IP ou nom de domaine complet du noeud 1>

Configurer les paramètres XMPP dans Web Admin

Sur chaque serveur avec le service CallBridge

30. Entrez cb1 sur callbridge1, etc.
31. Entrez le domaine : example.com
32. Entrez secret à partir du bloc-notes pour le pont d'a correspondant
33. Vérifier la page d'état de webadmin pour l'authentifi

l'authentification

Remarque 1 : l'approbation de cluster xmpp dans l'exemple est le certificat XMPP, car le certificat contient tous les FQDN du serveur XMPP dans l'attribut Subject Alternative Name (SAN) ou est un certificat générique. Si chaque serveur XMPP a son propre certificat, vous devez les combiner et les ajouter en tant que cluster de confiance xmpp.

Remarque 2 : xmpp callbridge add cb4. Ajouté cette étape comme exemple que vous pouvez avoir plus de ponts d'appel que de serveurs xmpp. Cette étape n'est pas nécessaire, mais a été ajoutée comme exemple.

Remarque 3 : xmpp callbridge ad-secret cb4. Ajout de cette étape pour aller de l'avant avec la note 2. Si vous avez 4 ponts d'appel, vous devez ajouter les 4 à tous les noeuds du cluster xmpp.

Si vous restez sur la version CMS 2.9.x, vous pouvez commencer les tests et la validation maintenant pour vous assurer que les nouveaux serveurs fonctionnent comme prévu.

Vérification

Après la migration vers les nouveaux serveurs, vérifiez que tous vos utilisateurs et espaces sont visibles et que vos appels SIP fonctionnent toujours. Si vous restez sur la version CMS 2.9.x, vérifiez que XMPP fonctionne toujours (les utilisateurs de WebRTC peuvent toujours se connecter/se connecter, l'enregistreur peut se connecter, etc). Vérifiez tous les serveurs qui communiquent avec CMS pour vous assurer qu'ils sont toujours fonctionnels (Cisco Meeting Manager (CMM), Cisco Unified Communications Manager (CUCM), TelePresence Management Suite (TMS), Expressway). Il est également recommandé d'exécuter 'syslog Follow' dans le MMP pour voir s'il y a des erreurs qui doivent être corrigées.

Dépannage

Si vous rencontrez des problèmes, vous pouvez revenir à vos serveurs de la gamme X ou contacter le TAC de Cisco pour obtenir de l'aide.