Reemplace los servidores de la serie X con el dispositivo Cisco Meeting Server o la máquina virtual

Contenido

Introducción

Este documento describe cómo sustituir de forma segura y fiable los servidores Acano serie X por máquinas virtuales (VM) Cisco Meeting Server (CMS), servidores CMS1000 o CMS2000. El soporte de servidores Acano serie X se ha descartado desde la versión 3.0 en adelante. El software más reciente que puede ejecutar en una serie X es 2.9.5, que sólo se admite hasta el 1 de marzo de 2022. Después de lo cual, no habrá más versiones de mantenimiento o correcciones de errores. Esto significa que si tiene un servidor Acano serie X, debe planear reemplazarlo antes de ese momento.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- administración de CMS
- Actualizaciones de CMS
- Creación y firma de certificados

Componentes Utilizados

La información de este documento se basa en los servidores Cisco Meeting Server (VM o CMS1K, o CMS2K) y Acano X-Series.

The information in this document was created from the devices in a specific lab environment. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Al sustituir los servidores de la serie X, debe tener en cuenta las capacidades de llamada de los distintos servidores. Consulte las guías de implementación de Cisco Meeting Server en el Apéndice C (https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html) para obtener orientación sobre el tamaño.

Tamaño de la serie X para referencia:

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

El proceso de configuración del servidor de reemplazo se puede encontrar en la documentación de instalación y no se trata a continuación. Las guías de instalación se pueden encontrar aquí: https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-guides-list.html.

Sustitución de servidores de la serie X por un dispositivo CMS o una máquina virtual

El método admitido para reemplazar los servidores de la serie X es agregar el nuevo dispositivo al clúster de base de datos para obtener una copia de la base de datos.

> **Precaución:** No utilice una copia de seguridad de un servidor de la serie X para implementar el reemplazo.

Para completar el reemplazo, no es necesario realizar todos los pasos siguientes. Agrupe sus nuevos servidores con los servidores antiguos para obtener una copia de la base de datos.

Una vez completado el proceso de migración, toda la información de la base de datos (reglas de entrada, reglas de salida, espacios compartidos, ID de llamada, etc.) también se encuentra en los nuevos servidores.

> **Nota:** Los datos introducidos en la interfaz gráfica de usuario (GUI) en **Configuration > General** and **Configuration > Active Directory** NO están en la base de datos. Debe mover la configuración LDAP (protocolo ligero de acceso a directorios) de la interfaz gráfica de usuario a la interfaz de programación de aplicaciones (API). Si todavía no está preparado para hacerlo, copie todos los datos de esas dos páginas para que se vuelvan a introducir en los nuevos servidores. Tenga en cuenta que la contraseña para el nombre de usuario LDAP también es necesaria para LDAP porque no puede copiar esa información.

Encontrará primero una descripción de alto nivel del flujo de trabajo, seguida de la instrucción paso a paso. Se recomienda seguir las instrucciones paso a paso para el procedimiento de reemplazo.

Descripción general del trabajo

Paso 1. Cree archivos de copia de seguridad desde servidores antiguos de la serie Acano X.

Paso 2. Descargue el archivo de copia de seguridad y el archivo logbundle.tar.gz de los

servidores antiguos en caso de que se necesite información para configurar el procesador de administración de placa base (MMP) del nuevo servidor.

Paso 3. En el servidor de la serie X anterior, inicie sesión en MMP y obtenga el resultado de cada servicio/configuración y copie la información en un archivo de nota.

Paso 4. Configurar nuevos servidores.

Paso 5. Obtenga licencias en los nuevos servidores.

Paso 6. Copie certificados de servidores antiguos a servidores nuevos.

Paso 7. Habilite los servicios MMP en los nuevos servidores configurados en el servidor antiguo. (La serie X de Acano puede utilizar una interfaz Admin dedicada para la administración. Debe administrar el nuevo servidor a través de la interfaz A-D, pero todos los servicios del nuevo servidor pueden estar en la interfaz A.)

Paso 8. Cree las mismas cuentas de usuario en los nuevos servidores que se utilizaron en los servidores antiguos.

Paso 9. Copie la base de datos en los nuevos servidores.

Paso 10. Elimine la serie X del clúster de base de datos.

Paso 11. Cierre el servidor de la serie X que reemplaza el nuevo servidor.

Paso 12. Cambie la IP en el nuevo dispositivo para que coincida con la antigua interfaz de la serie X A IP que se está reemplazando. Si utiliza varias interfaces en la serie X, también debe usarlas en los nuevos servidores, ya que esto elimina la necesidad de cambiar cualquier registro DNS.

Paso 13. Vuelva a unir el servidor al clúster de base de datos (sólo si la implementación original no era un único servidor combinado).

Paso 14. Ajuste los límites de carga en consecuencia en los nuevos servidores en la API - api/v1/system/configuration/cluster.

Paso 15. Pruebe la implementación para asegurarse de que sigue funcionando.

Instrucciones detalladas paso a paso

Paso 1. Cree una copia de seguridad utilizando el comando MMP **backup snapshot <server_specific_filename>**.

Paso 2. Descargue el archivo de copia de seguridad y un archivo logbundle.tar.gz (https://video.cisco.com/video/5810051601001) de cada uno de los servidores de la serie X que desea reemplazar.

Paso 3. Ejecute los siguientes comandos en los servidores de la serie X para obtener la configuración de los diversos servicios y ponerlos en un archivo de nota. Esto proporciona una referencia sencilla sobre cómo reconfigurar los nuevos servidores.

'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', v4 d', 'ipv4 admin', 'grabador', 'streaming', 'cargador', 'dscp', 'sipedge', 'h323_gateway', 'syslog', 'ldap'

> **Nota:** H323_gateway, Sip Edge y XMPP están obsoletos en CMS 3.0.
>
> Si utiliza SIP Edge, debe disponer de Cisco Expressway-C y E para enrutar el tráfico hacia y desde Internet.
> Si utiliza el gateway H323, debe configurarlo utilizando un servidor Cisco Expressway para realizar la interconexión H.323 a SIP.
> Si utiliza XMPP, una vez que actualice a CMS 3.x, deberá realizar algunos cambios en la configuración. Sin embargo, si está a punto de sustituir la serie X y permanecer en 2.9.x durante un tiempo, y necesita utilizar WebRTC, grabadora o optimizador, debe volver a configurar XMPP en su nuevo servidor.
>
> Puede leer más sobre los cambios que debe conocer antes de la actualización a CMS 3.0 en este documento.

Paso 4. Configure los nuevos servidores. Asegúrese de que tienen la misma versión de código que los servidores de la serie X. Dé a los servidores IP no usados que usar por ahora (**ipv4 <interface> add <address>/<prefix length> <gateway>**), pero cuando el trabajo se complete, las IP se cambian a lo que se utilizó en la serie X. Esto es para evitar cualquier cambio en los registros y certificados DNS. Si no desea reutilizar las IP antiguas, debe actualizar el DNS y los certificados en consecuencia.

Paso 5. En el nuevo servidor y el MMP del servidor de la serie X antiguo, ejecute el comando **iface a** para obtener la dirección MAC de las interfaces A. En la serie X que está a punto de ser reemplazada, descargue el archivo cms.lic y abra un caso de licencia del TAC. Dé al agente de licencias la nueva interfaz del servidor Dirección MAC A y la MAC del servidor antiguo y díganle que desea reemplazar el servidor antiguo por uno nuevo. Pídeles que cambien las licencias de la antigua MAC a la nueva MAC. A continuación, se proporciona un nuevo archivo de licencia que debe descomprimir, cambiar el nombre a cms.lic y cargar en el nuevo servidor.

Paso 6. Copie los certificados, las claves y los archivos de autoridad certificadora (CA) que se utilizan en la serie X antigua a los nuevos servidores mediante WinSCP o cualquier otro programa SFTP.

Paso 7. En el nuevo servidor, habilite los mismos servicios y configuraciones en MMP que tiene actualmente en su serie X anterior. Consulte la información recopilada en el paso 3 para asegurarse de que realiza las mismas configuraciones que antes.

> **Nota:** Si va a actualizar a CMS 3.x inmediatamente después de la configuración de estos nuevos servidores, no necesita configurar los componentes XMPP, Webbridge, SIP Edge o H323_gateway. Estos ya no se utilizan en CMS 3.x.

Paso 8. Cree las mismas cuentas de usuario que estaban en los servidores de la serie X en el MMP usando el comando **user add <username> <role>** (así como **user rule <rule name> <value>** si tiene alguna regla configurada). Se pueden configurar otros dispositivos como Cisco Meeting Management (CMM), TelePresence Management Suite (TMS) o Cisco Unified Communications Manager (CUCM) para las funciones con estas cuentas, por lo que debe asegurarse de configurarlos en los nuevos servidores.

Paso 9. Obtenga una copia de la base de datos en los nuevos servidores.

9a. Si la implementación actual es un único servidor combinado (sin clúster de base de datos), debe inicializar un clúster de base de datos en él. Desde la versión 2.7 de CMS en adelante, un clúster de base de datos requiere certificados. Por lo tanto, se ha introducido una autoridad de certificados integrada en CMS a partir de la versión 2.7 que puede utilizar para firmar los certificados de base de datos:

1. En el único MMP combinado de la serie X, ejecute **pki selfsigned dbca CN:<Nombre de la empresa>** (p. ej. pki selfsigned dbca CN:tplab.local)

2. En el único MMP combinado de la serie X, cree un certificado para el servidor de base de datos con **pki csr dbserver CN:xseries.example.com subjectAltName:<newcms1fqdn>**

(En este momento no es necesario tener registros A DNS para esto).

3. En el único MMP combinado de la serie X, cree un certificado para el cliente de base de datos con **pki csr dbclient CN:postgres**

4. En el único MMP combinado de la serie X, utilice dbca (desde el Paso 1) para firmar el certificado dbserver (desde el Paso 2) certificado **pki sign dbserver dbca**

5. En el único MMP combinado de la serie X, utilice dbca (desde el Paso 1) para firmar el certificado dbclient (desde el Paso 3) certificado **pki sign dbclient dbca**

6. Copie los archivos dbserver.crt, dbserver.key, dbclient.crt y dbclient.key a todos los servidores que se unirán a la base de datos (nodos que forman el clúster de base de datos) de la serie X a los nuevos servidores

7. Copie el archivo dbca.crt en todos los servidores de la serie X

8. En el único MMP combinado de la serie X, ejecute **database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt** (dbca.crt como certificado de CA raíz)

9. En el único MMP combinado de la serie X, ejecute **database cluster localnode a**

10. En el único MMP combinado de la serie X, ejecute el **clúster** de **base de datos inicializado**

11. En el único MMP combinado de la serie X, ejecute el **estado del clúster de la base de datos**. Debe ver:
Nodos: <XseriesIP> (me) : Principal conectado

12. En los nuevos servidores a los que se unirá al clúster de base de datos, desde MMP ejecute **los certificados de clúster de base de datos dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt**

13. En los nuevos servidores a los que se unirá (ubicados conjuntamente con una base de datos), desde MMP:

a. ejecutar **cluster localnode a de base de datos**

b. ejecute **database cluster Join <primary node IP>**

En este momento, los nuevos servidores tienen o tienen una copia de la base de datos. Ejecute **el estado del clúster de base de datos** en MMP en el nuevo servidor para asegurarse de que se muestren como sincronizados. Si lo están, ha terminado con el paso 9 y puede continuar con el paso 10. Sin embargo, si no están sincronizados, debe revisar las configuraciones del clúster de la base de datos y asegurarse de que no haya nada en la red que bloquee la comunicación sobre TCP 5432 entre los servidores.

9 ter. Si la implementación actual ya es un clúster de base de datos, desea reemplazar los servidores de la serie X uno por uno. En la serie X, ejecute en el **estado del clúster de base de datos** MMP para verificar si el servidor se une al clúster de base de datos o está conectado. Si la IP del servidor está en la lista de clústeres de base de datos, se une. Si no lo es, y el último comando mostrado es 'conexión del clúster de base de datos', entonces el nodo está conectado.

Desea volver a agregar el nuevo nodo con la misma función (conectada o unida), así que tenga en cuenta la función del servidor de la serie X. Si la serie X es la base de datos principal, reinicie el servidor primero para que se convierta en una réplica.

1. En la serie X que se va a sustituir, tenga en cuenta los certificados utilizados para la clave/certificado del servidor, la clave/certificado del cliente y el certificado CA

2. En la serie X que se va a reemplazar, ejecute **cluster de base de datos remove**

Paso 10. Si reemplaza un **único servidor combinado de la serie X**, continúe aquí con el paso 10. Si se trata de un clúster, vaya directamente al paso 11.

En este momento, el nuevo servidor tiene una copia de la base de datos. Puede confirmar esto con un inicio de sesión en la interfaz web del nuevo servidor y verificar la configuración de usuarios y espacios. Después de la confirmación, quite ahora el nuevo servidor del clúster de base de datos y cambie las IP:

1. En el nuevo servidor, ejecute '**cluster de base de datos remove**'.

2. Cierre el servidor de la serie X.

3. Cambie las IP del nuevo servidor por las que se utilizan en el servidor de la serie X.

4. Reinicie el nuevo servidor.

5. Si permanece en la versión 2.9.x de CMS, pruebe el nuevo servidor para asegurarse de que todas las configuraciones funcionen.

6. Inicie sesión en la página web admin del nuevo servidor y observe los espacios y usuarios. Debe ver todos los espacios y usuarios que estaban previamente en el servidor cuando se unieron a la base de datos anteriormente, ya que se necesitó una copia de ella.

Paso 11. Si reemplaza un servidor de la serie X que forma parte de un clúster, puede seguir los siguientes pasos:

1. Cierre el servidor de la serie X que pretendemos desactivar.

2. Cambie las IP del nuevo servidor a lo que se utilizaba anteriormente en la interfaz de nodo local de la base de datos del servidor de la serie X (normalmente, a).

3. Copie la clave/certificado del servidor, la clave/certificado del cliente y el certificado CA al nuevo servidor con un programa SFTP.

4. En el nuevo servidor, ejecute el comando: '**database cluster localnode a**'

5 bis. Si el nuevo nodo se va a unir al clúster de base de datos, ejecute el comando **database cluster certs <server.key> <server.crt> <client.key> <client.crt> <ca.crt>**'

5 ter. Si se va a conectar el nuevo nodo (que no se encuentra junto con una base de datos) al clúster de base de datos, ejecute el comando **database cluster certs <client.key> <client.crt> <ca.crt>**.

6 bis. Si el nuevo nodo necesita ser unido (ubicado conjuntamente con una base de datos) ejecute el comando: '**conexión del clúster de base de datos <IP del nodo primario>**'

6 ter. Si el nuevo nodo necesita estar conectado (no se encuentra junto con una base de datos) ejecute el comando: '**conexión del clúster de base de datos <IP del nodo primario>**'

Repita los pasos 9b y 11 para cada serie X que necesite retirar.

Paso 12. En este punto, los nuevos servidores CMS tendrán una copia de la base de datos, o si están conectados, sabrán cómo alcanzar los nodos de la base de datos y también tendrán las mismas direcciones IP que antes.

Paso 13. ¿Está activado el equilibrio de carga en su implementación?

Si utiliza el balanceo de carga de llamadas de CMS con CallBridgeGroups en la API configurada con Loadbalance=True, debe cambiar el límite de carga para que coincida con los límites recomendados de los nuevos servidores en el entorno. Vaya a **api/v1/system/configuration/cluster** y actualice el límite de carga en consecuencia:

Sistema	Límite de carga recomendado
CMS1000 M5v2	120000
CMS1000 M4 o M5v1	96000
CMS2000 M5v2	875000
CMS2000	700000
VM (número de vCPU x 1250)	ejemplo: 70 vCPU x 1250 = 87500

Paso 14. Si tuvo un clúster XMPP antes de este trabajo y pretende permanecer en CMS 2.9.x durante un tiempo, debe reconstruir el clúster XMPP.

Comandos MMP	Examples
Configurar en todos los nodos XMPP	**Configurar en todos los nodos XMPP**
1. restablecimiento de Xmpp	1. restablecimiento de Xmpp
2. xmpp domain <domain name>	2. xmpp domain example.com
3. xmpp hear <lista blanca de la interfaz>	3. xmpp hear 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 *** Nota 1
Configuración del primer nodo	**Configuración del primer nodo**
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>
10. xmpp callbridge add <callbridge name>
11. xmpp callbridge list
12. xmpp disable
13. xmpp cluster enable
14. xmpp cluster inicializar
15. xmpp enable
16. xmpp cluster status

Configuración de los nodos 2º y 3º

17. xmpp enable
18. xmpp callbridge add-secret <callbridge name>
19. ingrese callbridge secret:
20. xmpp callbridge add-secret <callbridge name>
21. Introduzca callbridge secret:
22. xmpp callbridge add-secret <callbridge name>
23. Introduzca callbridge secret:
24. xmpp callbridge add-secret <callbridge name>
25. Introduzca callbridge secret:
26. xmpp disable
27. xmpp cluster enable
28. xmpp enable
29. xmpp cluster Join <cluster>

Configuración de la configuración de XMPP en el administrador Web

En cada servidor con el servicio CallBridge

30. Introduzca este nombre único de callbridges configurado arriba
31. Introduzca el dominio
32. Introduzca el secreto del bloc de notas
33. Verifique la página de estado de webadmin para la autenticación

9. xmpp callbridge add cb3
10. xmpp callbridge add cb4 *** Nota 2
11. xmpp callbridge list <— copia este resultado en notepad
12. xmpp disable
13. xmpp cluster enable
14. xmpp cluster inicializar
15. xmpp enable
16. xmpp cluster status

Configuración de los nodos 2º y 3º

17. xmpp enable
18. xmpp callbridge add-secret cb1
19. Introduzca callbridge secret: <copy secret for cb from notepad>
20. xmpp callbridge add-secret cb2
21. Introduzca callbridge secret: <copy secret for cb from notepad>
22. xmpp callbridge add-secret cb3
23: Introduzca callbridge secret: <copy secret for cb from notepad>
24. xmpp callbridge add-secret cb4 *** Nota 3
25. Introduzca callbridge secret: <copy secret for cb from notepad>
26. xmpp disable
27. xmpp cluster enable
28. xmpp enable
29. xmpp cluster Join <dirección IP o FQDN del nod

Configuración de la configuración de XMPP en e administrador Web

En cada servidor con el servicio CallBridge

30. Introduzca cb1 en callbridge1, etc
31. Introducir dominio: example.com
32. Introduzca el secreto del bloc de notas para el callbridge correspondiente
33. Verifique la página de estado de webadmin para autenticación

Nota 1: xmpp cluster trust en el ejemplo es el certificado XMPP porque el certificado contiene todos los FQDN del servidor XMPP en el atributo Subject Alternative Name (SAN) o es un certificado comodín. Si cada servidor XMPP tiene su propio certificado, debe combinarlos y agregarlos como confianza de clúster xmpp.

Nota 2: xmpp callbridge add cb4. Se agregó este paso como ejemplo de que puede tener más callbridges de los que tiene servidores xmpp. Este paso no es necesario, pero se agregó como ejemplo.

Nota 3: xmpp callbridge ad-secret cb4. Se ha añadido este paso a la nota 2. Si tiene 4 callbridges, debe agregar los 4 a todos los nodos del clúster xmpp.

Si permanece en la versión 2.9.x de CMS, puede comenzar las pruebas y la validación ahora para asegurarse de que los nuevos servidores funcionen como se esperaba.

Verificación

Después de la migración a los nuevos servidores, compruebe que todos sus usuarios y espacios estén visibles y que las llamadas SIP sigan funcionando. Si se mantiene en la versión 2.9.x de CMS, confirme que XMPP sigue funcionando (los usuarios de WebRTC aún pueden conectarse/iniciar sesión, el grabador puede conectarse, etc). Compruebe los servidores que estén en comunicación con CMS para asegurarse de que siguen funcionando (Cisco Meeting Manager (CMM), Cisco Unified Communications Manager (CUCM), TelePresence Management Suite (TMS) y Expressway). También es una buena idea ejecutar 'syslog Follow' en el MMP para ver si hay algún error que se deba resolver.

Troubleshoot

Si tiene algún problema, puede volver a los servidores de la serie X o ponerse en contacto con el TAC de Cisco para obtener asistencia.