Dispositivo NAC (CCA): Alta disponibilidad de la configuración (HA) para el Access Manager limpio (CAM)

Contenido

Introducción

Este documento describe cómo configurar un par de máquinas limpias del Access Manager (CAM) para la Alta disponibilidad (HA). Cuando despliegan a los administradores limpios del acceso en el modo de gran disponibilidad, usted puede asegurarse de que la supervisión, la autenticación, y las tareas importantes de la información continúen en caso de inesperado apaguen.

Nota: Refiera a la sección de gran disponibilidad que configura (HA) del dispositivo NAC de Cisco - instalación y guía de administración limpias del servidor de acceso (CAS) para saber configurar

la característica HA en CAS.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el dispositivo del Cisco Network Admission Control (NAC) - versión 4.1 CAM.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Información general

Estos puntos claves proporcionan un resumen de alto nivel de operación HA-CAM:

1. El modo de gran disponibilidad del Access Manager limpio es una configuración activa/pasiva del dos-servidor en la cual una máquina espera CAM actúa como respaldo a una máquina activa CAM.
2. El Access Manager limpio activo realiza todas las tareas para el sistema. El CAM espera monitorea el CAM activo y mantiene su base de datos sincronizada con la base de datos activa CAM.
3. Ambos CAM comparten un IP virtual del servicio para la interfaz confiada en eth0. El Domain Name se debe utilizar para el certificado SSL.
4. Las máquinas primarias y secundarias CAM intercambian los paquetes de latidos UDP cada 2 segundos. Si expira el temporizador Heartbeat (de latido), la falla de estado ocurre.
5. La interfaz y/o la interfaz serial del eth1 en los CAM se pueden utilizar para los paquetes de latidos y la sincronización de la base de datos. Si el eth1 y las interfaces seriales se configuran para el latido del corazón, ambas interfaces necesitan no poder para que la Conmutación por falla ocurra.

El modo de gran disponibilidad del Access Manager limpio es una configuración activa/pasiva del dos-servidor en la cual una máquina limpia espera del Access Manager actúa como respaldo a una máquina limpia activa del Access Manager. Mientras que el CAM activo lleva la mayor parte de la carga de trabajo en condiciones normales, los monitores inactivos el CAM activo y guardan su almacén de datos sincronizaron con los datos del CAM activo.

Si ocurre un evento de falla, por ejemplo si el CAM activo apaga o no responde a la señal del “latido del corazón” del par, el recurso seguro asume el papel del CAM activo.

Cuando usted primero configura a los pares HA, usted debe especificar un CAM HA-primario y el CAM HA-secundario. Inicialmente, el HA-primario es el CAM activo, y el HA-secundario es el CAM (pasivo) espera, pero los papeles activos/pasivos no se asignan permanentemente. Si va el CAM primario abajo, el secundario (espera) se convierte en el CAM activo. Cuando los reinicios del primario original CAM, él asumen el papel de reserva.

Cuando el Access Manager limpio empieza para arriba, marca para ver si su par es activo. Si no, el CAM que empieza para arriba asume rol activo. Si el par es activo, por otra parte, el CAM que comienza se convierte en el recurso seguro.

Usted puede configurar a dos administradores limpios del acceso como par HA al mismo tiempo, o usted puede agregar un nuevo Access Manager limpio a un CAM independiente existente para crear un par de gran disponibilidad. Para que los pares aparezcan a la red y al Access Servers limpio como una entidad, usted debe especificar una dirección IP del servicio que se utilizará como el direccionamiento de confianza de la interfaz (eth0) para los pares HA.

Para crear la red de la cruce en la cual se intercambia la información de gran disponibilidad, usted conecta los puertos del eth1 de ambos CAM y especifica a una dirección de red privada ruteada no no actualmente en su organización (la red de la cruce del valor por defecto el HA es 192.168.0.252). El Access Manager limpio entonces crea una red privada, segura, del dos-nodo para los puertos del eth1 de cada CAM para intercambiar el tráfico del latido del corazón UDP y para sincronizar las bases de datos. Observe que el CAM utiliza siempre el eth1 como la interfaz del latido del corazón UDP.

Para la Seguridad adicional, usted puede también conectar los puertos seriales de cada Access Manager limpio para el intercambio del latido del corazón. En este caso, el latido del corazón UDP y las interfaces seriales del latido del corazón deben no poder para que el sistema inactivo asuma el control.

Nota: Para la conexión de cable serial para el HA (HA-CAM o HA-CAS), el cable serial debe ser un cable del “módem nulo”.

Requisitos básicos antes de que usted proceda

Advertencia: Para prevenir cualquier pérdida de datos posible dentro de la sincronización de la base de datos, aseegurese siempre que el Access Manager limpio (secundario) espera esté vivo antes de fallar sobre el Access Manager limpio (primario) activo.

Antes de que usted configure la Alta disponibilidad, asegúrese de que usted cumpla estos requisitos:

1. Usted ha obtenido una licencia de gran disponibilidad (de la Conmutación por falla).**Nota:** Cuando usted instala una licencia de la Conmutación por falla CAM (HA), instale la licencia de la Conmutación por falla al CAM primario primero, después cargue el resto de licencias. Las licencias independientes se pueden también utilizar para la Alta disponibilidad.
2. Ambos CAM están instalados y configurados.
3. Para el latido del corazón, cada CAM necesita tener un nombre de host único (o Nombre del nodo). Para los pares HA CAM, este nombre del host se proporciona al par y se debe resolver con el DNS o agregar a /etc/hosts el archivo del par.

4. Usted tiene a certificado firmado por CA para el Domain Name de los pares HA CAM.
5. El CAM HA-primario es de configuración completa para la operación del tiempo de ejecución. Esto significa que las conexiones a las fuentes de la autenticación, las directivas, los rol del usuario, los Puntos de acceso, y así sucesivamente, son todas especificados. Esta configuración se duplica automáticamente en el CAM (espera) HA-secundario.
6. Ambo limpie a los administradores del acceso son accesible en la red (intento para hacerlos ping para probar la conexión).
7. Las máquinas en las cuales el software CAM está instalado tienen un acceso de Ethernet libre (eth1) y por lo menos un puerto serial libre. Utilice los manuales de la especificación para que el hardware del servidor identifique el puerto serial (ttyS0 o ttyS1) en cada máquina.
8. En las implementaciones fuera de banda, la Seguridad de puerto no se habilita en las interfaces del switch con las cuales CAS y el CAM están conectados. Esto puede interferir con la salida de CAS HA y del DHCP.

Estos procedimientos le requieren reiniciar el Access Manager limpio. En aquel momento, sus servicios son abreviadamente inasequibles. Configure un CAM en línea cuando el tiempo muerto tiene el menos impacto en sus usuarios.

Nota: Las consolas del administrador Web del dispositivo NAC de Cisco apoyan al Internet Explorer 6.0 o sobre el navegador.

Conecte las máquinas limpias del Access Manager

Hay dos tipos de conexión entre los pares HA-CAM: uno para intercambiar los datos del tiempo de ejecución que se relacionan con las actividades y la limpia el Access Manager para la señal de prueba SQE. En la Alta disponibilidad, el Access Manager limpio utiliza siempre la interfaz del eth1 para el intercambio de datos y el intercambio del latido del corazón UDP. Cuando la señal de prueba SQE UDP no puede ser transmitida y ser recibida dentro de cierto período de tiempo, el sistema inactivo asume el control. Para proporcionar una medida adicional de Seguridad, se recomienda altamente para agregar una conexión de latido serial entre los pares limpios del Access Manager. La conexión en serie proporciona un método dedicado adicional del intercambio del latido del corazón que deba fallar antes de que el sistema inactivo pueda asumir el control. Observe que la conexión del eth1 entre los pares CAM es obligatoria.

Conecte físicamente a los administradores limpios del acceso del par como se muestra:

- Utilice el cable de par cruzado para conectar los accesos de Ethernet del eth1 de las máquinas limpias del Access Manager. Esta conexión se utiliza para la interfaz y el intercambio de datos (Reflejo del latido del corazón UDP de la base de datos) entre los pares de la Conmutación por falla.
- Utilice el cable serial del módem nulo para conectar los puertos seriales (recomendados altamente). Esta conexión se utiliza como intercambio serial del latido del corazón adicional (señal de mantenimiento) entre los pares de la Conmutación por falla.

Nota: Para la conexión de cable serial para el HA (HA-CAM o HA-CAS), el cable serial debe ser un cable del “módem nulo”.

Conexión en serie

Si la máquina que funciona con el software limpio del Access Manager tiene dos puertos seriales,

usted puede utilizar el puerto adicional para la conexión de latido serial. Por abandono, el primer puerto serial detectado en el servidor CAM se configura para la entrada-salida de la consola (facilitar la instalación y otros tipos de acceso administrativo).

Si la máquina tiene solamente un puerto serial (COM1 o ttyS0), usted puede configurar de nuevo el puerto para servir como la conexión de latido de gran disponibilidad. Esto es porque, después de que el software CAM esté instalado, la consola de SSH o KVM se puede utilizar siempre para acceder la interfaz de línea de comando del CAM.

Usted puede habilitar/neutralización el puerto serial con la casilla de verificación **serial del login de la neutralización** en las configuraciones HA CAM (bajo **administración > Access Manager limpio > red y Conmutación por falla | Configuraciones de la Conmutación por falla | Login serial de la neutralización**). Cuando hay solamente un puerto serial en la máquina CAM, esta casilla de verificación permite que los administradores inhabiliten el login serial en el COM1 para poderla utilizar como la interfaz serial del latido del corazón para un par de administradores HA-limpios del acceso.

Nota: El login serial **se habilita** por abandono en el CAM. Si usted utiliza el COM1 para la interfaz serial del latido del corazón del CAM, usted debe hacer clic la casilla de verificación **serial del login de la neutralización** para inhabilitar el login serial en el COM1.

Configure el CAM HA-primario

Una vez que usted ha verificado los requisitos previos, realice estos pasos para configurar el Access Manager limpio como el HA-primario para los pares de gran disponibilidad. Vea la figura para un ejemplo de la configuración de muestra.

1. Abra la consola del administrador Web para que el Access Manager limpio sea señalado como el HA-primario, y vaya a la **administración > CCA administrador > certificado SSL** para configurar el certificado SSL para el CAM primario. La forma **temporal del certificado de la generación** aparece.**Nota:** Los pasos para la configuración HA en este documento asumen que un certificado temporal está exportado del CAM HA-primario al CAM HA-secundario.*Si usted utiliza un certificado temporal para los pares HA, realice estos pasos:*Llene el formulario **temporal el certificado de la generación** y el tecleo **genera**. El certificado se debe generar para el Domain Name de los pares HA.Después de que usted genere el certificado temporal, elija la **clave/el certificado de la exportación CSR/Private del elegir un Menú Action (Acción)**.Haga clic el botón de la **exportación** para que la **clave privada actualmente instalada** exporte la clave privada SSL. Salve el archivo clave al disco. Usted tiene que importar esta clave en el CAM HA-secundario más adelante.Haga clic el botón de la **exportación** para que el **certificado actualmente instalado** exporte el certificado actual SSL. Salve el archivo de certificado al disco. Usted tiene que importar este archivo de certificado en el CAM HA-secundario más adelante.*Si usted utiliza a certificado firmado por CA para los pares HA, realice estos pasos:***Nota:** Certificado firmado por CA debe ser basado en el Domain Name resolvable al IP del servicio con el DNS. Refiérase manejan los Certificados CAM SSL bajo sección de la administración en el dispositivo NAC de Cisco - instalación y guía de administración CAM para más información.Elija **Import Certificate (Importar certificado) del elegir un Menú Action (Acción)**.Utilice el **botón Browse** al lado del campo del **archivo de certificado** y navegue al certificado firmado por CA.Choose CA-**firmó CERT PEM-codificado X.509 del** menú desplegable del **tipo de archivo**.**Carga del** tecleo para importar el certificado.

Observe que usted necesita importar este mismo certificado en el CAM HA-secundario más adelante.El tecleo **verifica y instala los Certificados cargados**.Elija la **clave/el certificado de la exportación CSR/Private del elegir una** lista desplegable de la **acción**.Haga clic el botón de la **exportación** para que la **clave privada actualmente instalada** exporte la clave privada SSL asociada al certificado firmado por CA. Salve el archivo clave al disco. Usted necesita importar este archivo en el CAM HA-secundario más adelante.

2. Va a la **administración > CCA el administrador** y hace clic la **red y la Conmutación por falla** cuadro elige la opción HA-**primaria del** menú desplegable **de gran disponibilidad del modo**. Las configuraciones de gran disponibilidad aparecen.
3. Copie el valor del campo del **IP Address** bajo **configuraciones de red** y ingreselo en el campo del **IP Address del servicio**. La dirección IP de las configuraciones de red es la dirección IP existente del Access Manager limpio actual. La idea aquí es dar vuelta a esta dirección IP, que el Access Servers limpio reconoce ya, en la dirección IP virtual del servicio para los pares limpios del Access Manager.
4. Cambie la dirección IP bajo **configuraciones de red a una** dirección disponible, por ejemplo, n.152.
5. Cada Access Manager limpio debe tener un nombre del host único, tal como camanager1 y camanager2. Teclee el nombre del host del CAM HA-primario en el campo de **nombre del host** bajo **configuraciones de red**, y teclee el nombre del host del CAM HA-secundario en el campo de **nombre del host del par** bajo **configuraciones de la Conmutación por falla**.Un valor del **nombre del host** es obligatorio cuando usted configura la Alta disponibilidad, mientras que el **Domain Name del host** es opcional.Los campos del **nombre del host** y de **nombre del host del par** son con diferenciación entre mayúsculas y minúsculas. Aseegurese hacer juego qué se teclea aquí con lo que se teclea para el CAM HA-secundario más adelante.
6. Del menú desplegable de la **interfaz serial del latido del corazón**, elija el puerto serial con el cual usted conectó el cable serial del CAM HA-primario, o deje este n/a si usted no utiliza una conexión en serie.
7. Si su máquina tiene solamente un puerto serial y usted utiliza el COM1 como la interfaz serial del latido del corazón, usted debe marcar la casilla de verificación **serial del login de la neutralización** para asegurarse de que el login serial está inhabilitado en el COM1. Vea la conexión en serie para otros detalles.
8. Para mantener la sincronización, el Access Manager limpio mira los intercambiares datos por una red de la cruce. Usted debe especificar un espacio de dirección de red privada ruteado no no actualmente en su organización en el **campo de red de la cruce**, tal como 10.10.10. La red predeterminada de la cruce proporcionada es 192.168.0.252. Si este los conflictos de dirección con su red, se aseeguran especificar un diverso espacio de dirección privada. Por ejemplo, si su organización utiliza la red privada 192.168.151.0, uso 10.1.1.x como la red de la cruce. Reparan, ingresa tan solamente al octeto de la máscara de subred y del último del IP Address la porción de la red del IP Address en el **campo de red de la cruce**.
9. Haga clic la **actualización** y después **reinicie** para recomenzar el Access Manager limpio.Después de los reinicios limpios del Access Manager, aseegurese que la máquina CAM funciona correctamente. Marque para ver si el Access Servers limpio está conectado y autentican a los usuarios nuevos.

Configure el CAM HA-secundario

Realice estos pasos para configurar el CAM HA-secundario.

1. Abra la consola del administrador Web para que el Access Manager limpio sea señalado como el HA-secundario, y vaya a la **administración > CCA administrador > certificado SSL**.
2. Antes de que usted proceda, realice estos pasos:Sostenga la clave privada del CAM secundario.Aseegurese la clave privada y los archivos de certificado SSL asociados al servicio IP/HA-Primary CAM están disponibles (exportado previamente según lo descrito adentro configure el CAM HA-primario).
3. Importe el archivo de clave privado y el certificado del CAM HA-primario según lo descrito:En la lengueta del **certificado SSL**, elija **Import Certificate (Importar certificado) del elegir un Menú Action (Acción)**.El tecleo **hojea** al lado del campo del **archivo de certificado**, y hojea a su copia de backup del archivo de clave privado generado con el certificado que se utiliza para los pares HA.Elija la **clave privada** como el tipo de archivo.Haga clic la **carga** para cargar la clave privada.Con **Import Certificate (Importar certificado)** elegido del **elegir un Menú Action (Acción)**, hojee al certificado (temporal o CA-firmado) que se asocia a la clave privada.Choose CA-**firmó CERT PEM-codificado X.509** como el tipo de archivo.Haga clic la **carga** para cargar el certificado temporal o certificado firmado por CA.El tecleo **verifica y instala los Certificados cargados**.Refiérase manejan los Certificados CAM SSL bajo sección de la administración en el dispositivo NAC de Cisco - instalación y guía de administración CAM para más información.
4. Van a la **administración > CCA el administrador > la red y la Conmutación por falla | Las configuraciones de red** y cambian la dirección IP del CAM secundario a un direccionamiento que sea diferente de la dirección IP HA-primaria CAM y de la dirección IP del servicio.
5. Fije el valor del **nombre del host** bajo **configuraciones de red al** mismo valor establecidovalor establecido para el **nombre del host del par** en la configuración HA-primaria CAM. Vea la figura en la sección primaria HA.**Nota:** Los campos del **nombre del host** y de **nombre del host del par** son con diferenciación entre mayúsculas y minúsculas. Aseegurese hacer juego qué se teclea aquí con lo que fue tecleado para el CAM HA-primario.
6. Elija HA-**secundario** en el menú desplegable **de gran disponibilidad del modo**. La Alta disponibilidad de las configuraciones aparece.
7. Fije el valor de la **dirección IP del servicio** bajo **configuraciones de la Conmutación por falla al** mismo valor establecidovalor establecido para la **dirección IP del servicio** en la configuración HA-primaria CAM.
8. Fije el valor del **nombre del host del par** bajo **configuraciones de la Conmutación por falla al** nombre del host del CAM HA-primario.
9. Del menú desplegable de la **interfaz serial del latido del corazón**, elija el puerto serial con el cual usted conectó el cable serial del CAM HA-primario, o deje este n/a si usted no utiliza una conexión en serie.
10. Si su máquina tiene solamente un puerto serial y usted utiliza el COM1 como la interfaz serial del latido del corazón, usted debe marcar la casilla de verificación **serial del login de la neutralización** para asegurarse de que el login serial está inhabilitado en el COM1. Vea la conexión en serie para otros detalles.
11. Teclee las mismas configuraciones de la **interfaz de la red de la cruce** que usted había ingresado para el CAM HA-primario.
12. Haga clic la **actualización** y después **reinicie**.

Cuando el CAM espera empieza para arriba, sincroniza automáticamente su base de datos con el CAM activo.

Finalmente, abra la consola admin para el recurso seguro otra vez y complete la configuración. Note que la consola admin para el recurso seguro ahora tiene solamente un módulo de administración.

Complete la configuración

Verifique las configuraciones en la página de la **red y de la Conmutación por falla** para el CAM espera.

La configuración de alta disponibilidad es completa ahora.

El fallar sobre un par HA-CAM

Advertencia: Para prevenir cualquier pérdida de datos posible dentro de la sincronización de la base de datos, aseegurese siempre que el CAM espera esté vivo antes de fallar sobre el CAM activo.

Para la Conmutación por falla a los pares HA-CAM, SSH a la máquina activa en los pares y realiza uno de estos comandos:

- **apague** o
- **reinicie** o
- **mantenga la parada del perfigo**Esto para todos los servicios en la máquina activa. Cuando el latido del corazón falla, la máquina espera asume rol activo. Realice el **comienzo del perfigo del servicio** para recomenzar los servicios en la máquina parada. Esto hace la máquina parada asumir la rol en espera.**Nota: el reinicio del perfigo del servicio** no se debe utilizar para probar la Alta disponibilidad (Conmutación por falla). En lugar, Cisco recomienda **apaga** o **reinicia** en la máquina para probar la Conmutación por falla o los comandos CLI, la **parada del perfigo del servicio** y el **comienzo del perfigo del servicio**.

Comandos CLI útiles para el HA

Éstos son directorios útiles a saber para el HA en el CAM:

- `/etc/ha.d/perfigo/conf`
- `/etc/ha.d/ha.cf`

Este ejemplo muestra la ubicación del debug/de los archivos del registro HA, así como el nombre de cada CAM (nodo) en los pares HA:

```
[root@cam1  ha.d]#more ha.cf # Generated by make-hacf.pl udpport 694 bcast eth1 auto_failback
off apiauth default uid=root log_badpack false debug 0 debugfile /var/log/ha-debug logfile
/var/log/ha-log #logfacility local0 watchdog /dev/watchdog keepalive 2 warntime 10 deadtime 15
node cam1 node cam2
```

Cómo verificar el estado de tiempo de ejecución activo/espera en el HA CAM

Este ejemplo muestra cómo utilizar el CLI para determinar el estado de tiempo de ejecución (activo o espera) de cada CAM en los pares HA. Usted puede encontrar generalmente el comando de **fostate.sh del** directorio de /store de su actualización más reciente, por ejemplo, `/store/cca_upgrade-4.x.x.`

1. Ejecute el script de **fostate.sh** en el primer CAM:`[root@cam1 cca_upgrade-4.x.x]# ./fostate.sh`
   My node is active, peer node is standby [root@cam1 cca_upgrade-4.x.x]# *!--- This CAM is the active CAM in the HA-pair*
2. Ejecute el script de **fostate.sh** en el segundo CAM:`root@cam2 cca_upgrade-4.x.x]# ./fostate.sh`
   My node is standby, peer node is active [root@cam2 cca_upgrade-4.x.x]# *!--- This CAM is the standby CAM in the HA-pair*

Cómo verificar el estado de la configuración primario/secundario en el HA CAM

Este ejemplo muestra cómo utilizar el CLI para determinar el modo HA (primario/secundario) para cuál fue configurado cada CAM inicialmente en los pares HA.

1. Encuentre el nombre de los CAM (Nodos) con `/etc/ha.d/ha.cf.`
2. Entonces marque el estatus en cada CAM, por ejemplo:
```
[root@cam1 ~]# /perfigo/control/bin/check-ha cam1
active
[root@cam1 ~]# /perfigo/control/bin/check-ha cam2
active
```
3. Va a `/perfigo/control/tomcat y realiza el ls - el la`.Si los webapps señalan a **normal-webapps**, es el CAM primario.Si los webapps señalan al **admin-webapps**, es el CAM secundario.Por ejemplo, este CAM es el CAM primario:
```
[root@cam1 tomcat]# cd /perfigo/control/tomcat
[root@cam1 tomcat]# ls -la
total 216
drwxr-xr-x12 root root4096 Sep 14 23:28 .
drwxr-xr-x8 root root4096 Aug 28 22:12 ..
drwxr-xr-x4 root root4096 Aug 28 22:12 admin-webapps
<output cut…..>
drwxr-xr-x2 root root4096 Aug 28 22:12 temp
lrwxrwxrwx1 root root38 Sep 14 23:28 webapps -> /perfigo/control/tomcat/normal-webapps drwxr-xr-x 3 root root 4096 Aug 28 15:15 work
```
Este CAM es el CAM secundario:
```
[root@cam2 tomcat]# ls -la
total 216
drwxr-xr-x12 root root4096 Sep 14 23:33 .
drwxr-xr-x8 root root4096 Sep 152006 ..
drwxr-xr-x4 root root4096 Sep 152006 admin-webapps
<output cut …>
drwxr-xr-x2 root root4096 Sep 152006 temp
lrwxrwxrwx1 root root37 Sep 14 23:33 webapps -> /perfigo/control/tomcat/admin-webapps
drwxr-xr-x 3 root root 4096 Sep 14 23:25 work
```

Troubleshooting

Problema 1

Un error ocurre en CAM **“SSKEY en el servidor no hace juego el valor en la base de datos”** cuando CAS secundario en los pares HA llega a ser activo.

Solución

Resuelva este problema cuando usted avanza manualmente CAS primario SSKEY el secundario (botón de la restauración SSKEY, o invalidación manual en el archivo de /etc/.GUSSK en CAS).

Generalmente, este problema ocurre cuando usted substituye un dispositivo y no lo hace delete/re-add él desde/hasta el CAM. En este caso, CAS tiene su propio SSKEY basado en su dirección MAC y no hace juego posiblemente el que está fijado previamente en el CAM. Esto es especialmente verdad para CAS secundario porque tiene un SSKEY basado en su propia dirección MAC. En la configuración HA, incluso la secundaria tiene que utilizar CAS primario SSKEY basado en CAS primario MAC.

Problema 2

¡En los pares de la Conmutación por falla CAM, el CAM primario muestra la `ADVERTENCIA! ¡Conexiones cerradas a mirar base de datos del [x.x.x.x] (IP Address en Standby)! ¡Recomience por favor el nodo del peer para traer las bases de datos adentro sincronizan!!.`

Solución

Cuando se ha desconectado el link primario del eth1 y solamente sigue habiendo el link serial, el CAM vuelve un error en la base de datos que indique que no puede sincronizar con sus contrapartes HA, y el administrador ve este error en la consola Web CAM: .

```
WARNING! Closed connections to peer [standby
 IP] database! Please restart peer node to bring databases in
 sync!!
```

Utilice los Certificados uno mismo-firmados o de tercera persona en los pares CAM para resolver este problema.

Problema 3

Cómo cambiar la dirección IP para la Alta disponibilidad en el CAM

Solución

Intente derribar el CAM secundario con la **parada del perfigo del servicio**. Esta manera, no dirige los servicios del perfigo, sino que es todavía accesible por SSH. En el CAM primario, cambie el IP en la **administración > CCA administrador > red**. No la deje reiniciar todavía. Entonces vaya a la lengueta de la Conmutación por falla, y cambie la dirección IP del servicio. Después de este paso, entonces reinicielo.

Una vez que está completamente para arriba, aseegurese lo es accesible. Entonces ejecute el **comienzo del perfigo del servicio** en el CAM secundario, y realice los mismos cambios que usted hizo al primario. Entonces, reinicielo, y debe subir como el secundario. Para el CERT SSL, si se publica a un nombre, después cambie la entrada DNS de modo que el nombre resuelva al nuevo IP del servicio. Si se publica al IP, regenere un nuevo certificado temporal. En este momento, usted quiere probablemente tener un login del usuario a prueba. Si eso tiene éxito, la Conmutación por falla al secundario, y se aseegura le puede también iniciar sesión.

Información Relacionada

- Página de soporte del dispositivo NAC de Cisco
- Soporte Técnico y Documentación - Cisco Systems