Ferramenta NAC (CCA): Configurar a Alta disponibilidade (HA) para o Access Manager limpo (o CAM)

Índice

Introdução

Este documento descreve como estabelecer um par de máquinas limpas do Access Manager (CAM) para a Alta disponibilidade (HA). Quando os gerentes limpos do acesso são distribuídos na Alta disponibilidade do modo, você pode assegurar-se de que a monitoração, a autenticação, e as tarefas importantes do relatório continuem no caso de uma parada programada inesperada.

Nota: Refira a Alta disponibilidade configurando (HA) da seção da ferramenta NAC de Cisco - a instalação e Guia de Administração limpos do servidor de acesso (CAS) a fim saber configurar a característica HA em CAS.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no dispositivo do Cisco Network Admission Control (NAC) - versão 4.1 CAM.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Visão geral

Estes pontos chaves fornecem um sumário de nível elevado da operação HA-CAM:

1. A Alta disponibilidade limpa do modo do Access Manager é configuração de dois-server ativa/passiva em que uma máquina à espera CAM atua como um backup a uma máquina ativa CAM.
2. O Access Manager limpo ativo executa todas as tarefas para o sistema. O CAM à espera monitora o CAM ativo e mantém seu base de dados sincronizado com o base de dados ativo CAM.
3. Ambos os CAM compartilham de um IP virtual do serviço para a relação confiada eth0. O Domain Name deve ser usado para o certificado SSL.
4. As máquinas preliminares e secundárias CAM trocam pacotes de heartbeat UDP cada 2 segundos. Se o temporizador ritmado expira, a comutação classificada ocorre.
5. A relação eth1 e/ou a interface serial nos CAM podem ser usadas para pacotes de heartbeat e sincronização de base de dados. Se eth1 e as interfaces serial são configurados para a pulsação do coração, ambas as relações precisam para que o Failover não ocorra.

A Alta disponibilidade limpa do modo do Access Manager é configuração de dois-server ativa/passiva em que uma máquina limpa à espera do Access Manager atua como um backup a uma máquina limpa ativa do Access Manager. Quando o CAM ativo levar a maioria da carga de trabalho em condições normais, os monitores em standby o CAM ativo e mantêm sua loja dos dados sincronizaram com os dados do CAM ativo.

Se um evento do Failover ocorre, como se o CAM ativo fechou ou não respondeu ao sinal da “pulsação do coração” do par, o apoio supõe o papel do CAM ativo.

Quando você configura primeiramente os pares HA, você deve especificar um CAM HA-preliminar e o CAM HA-secundário. Inicialmente, o HA-preliminar é o CAM ativo, e o HA-secundário é o CAM (passivo) à espera, mas o active/papéis passivos não é atribuído permanentemente. Se o CAM preliminar vai para baixo, o secundário (à espera) transforma-se o CAM ativo. Quando o primário original CAM reinicia, supõe o papel alternativo.

Quando o Access Manager limpo começa acima, verifica para ver se seu par é ativo. Se não, o CAM que começa acima supõe o papel ativo. Se o par é ativo, por outro lado, o CAM que começa transforma-se o apoio.

Você pode configurar dois gerentes limpos do acesso como um par HA ao mesmo tempo, ou você pode adicionar um Access Manager limpo novo a um CAM autônomo existente para criar uma Alta disponibilidade dos pares. Para que os pares apareçam à rede e aos servidores de acesso limpos como uma entidade, você deve especificar um endereço IP de Um ou Mais Servidores Cisco ICM NT do serviço a ser usado como o endereço confiado da relação (eth0) para os pares HA.

A fim criar a rede do cruzamento em que a Alta disponibilidade da informação é trocada, você conecta as portas eth1 de ambos os CAM e especifica um endereço de rede privada distribuído não atualmente em sua organização (a rede do cruzamento do padrão o HA é 192.168.0.252). O Access Manager limpo cria então uma rede privada, segura, do dois-nó para as portas eth1 de cada CAM para trocar o tráfego da pulsação do coração UDP e para sincronizar bases de dados. Note que o CAM usa sempre eth1 como a relação da pulsação do coração UDP.

Para a Segurança extra, você pode igualmente conectar as portas serial de cada Access Manager limpo para a troca da pulsação do coração. Neste caso, a pulsação do coração UDP e as relações de série da pulsação do coração devem para que o sistema em standby não tome sobre.

Nota: Para a conexão de cabo serial para o HA (HA-CAM ou HA-CAS), o cabo serial deve ser um cabo do “modem nulo”.

Requisições básico antes que você continuar

aviso: A fim impedir toda a perda de dados possível dentro da sincronização de base de dados, certifique-se sempre de que o Access Manager limpo (secundário) à espera está vivo antes de falhar sobre o Access Manager limpo (preliminar) ativo.

Antes que você configure a Alta disponibilidade, assegure-se de que você cumpra estas exigências:

1. Você obteve uma Alta disponibilidade (Failover) da licença.**Nota:** Quando você instala uma licença do Failover CAM (HA), instale a licença do Failover ao CAM preliminar primeiramente, a seguir carregue todas as licenças restantes. As licenças autônomas podem igualmente ser usadas para a Alta disponibilidade.
2. Ambos os CAM são instalados e configurados.
3. Para a pulsação do coração, cada CAM precisa de ter um hostname original (ou o nome de nó). Para pares HA CAM, este nome de host é fornecido ao par e deve ser resolved com o DNS ou ser adicionado a /etc/hosts o arquivo do par.
4. Você tem um certificado assinado CA para o Domain Name dos pares HA CAM.
5. O CAM HA-preliminar é configurado inteiramente para a operação do tempo de execução.

Isto significa que as conexões às fontes da autenticação, políticas, papéis de usuário, os Access point, e assim por diante, são todas especificados. Esta configuração é duplicada automaticamente no CAM (à espera) HA-secundário.

6. Ambo limpe gerentes do acesso são acessível na rede (tentativa para os sibilar para testar a conexão).
7. As máquinas em que o software CAM é instalado têm uma porta Ethernet livre (eth1) e pelo menos uma porta serial livre. Use os manuais da especificação para que o hardware do servidor identifique a porta serial (ttyS0 ou ttyS1) em cada máquina.
8. Em disposições fora da banda, a Segurança de portas não é permitida nas interfaces de switch a que CAS e o CAM são conectados. Isto pode interferir com a entrega de CAS HA e DHCP.

Estes procedimentos exigem-no recarregar o Access Manager limpo. Naquele tempo, seus serviços são momentaneamente não disponíveis. Configurar um CAM em linha quando o tempo ocioso da máquina tem menos impacto em seus usuários.

Nota: Os consoles do admin da Web da ferramenta NAC de Cisco apoiam o internet explorer 6.0 ou acima do navegador.

Conecte as máquinas limpas do Access Manager

Há dois tipos de conexão entre pares HA-CAM: um para trocar os dados do tempo de execução que se relacionam às atividades e à limpas do Access Manager para o sinal ritmado. Na Alta disponibilidade, o Access Manager limpo usa sempre a relação eth1 para o intercâmbio de dados e a troca da pulsação do coração UDP. Quando o sinal ritmado UDP não transmite e não recebe dentro de um determinado período de tempo, o sistema em standby toma sobre. A fim fornecer uma medida extra da Segurança, é altamente recomendado adicionar uma conexão heartbeat de série entre os pares limpos do Access Manager. A conexão serial fornece um método dedicado adicional da troca da pulsação do coração que deva falhar antes que o sistema em standby possa tomar sobre. Note que a conexão eth1 entre os pares CAM é imperativa.

Conecte fisicamente os gerentes limpos do acesso do par como mostrado:

- Use o cabo crossover para conectar as portas Ethernet eth1 das máquinas limpas do Access Manager. Esta conexão é usada para a relação da pulsação do coração UDP e o intercâmbio de dados (Espelhamento do base de dados) entre os pares do Failover.
- Use o cabo serial do modem nulo para conectar as portas serial (altamente recomendados). Esta conexão é usada como uma troca de série da pulsação do coração adicional (manutenção de atividade) entre os pares do Failover.

Nota: Para a conexão de cabo serial para o HA (HA-CAM ou HA-CAS), o cabo serial deve ser um cabo do “modem nulo”.

Conexão serial

Se a máquina que executa o software limpo do Access Manager tem duas portas serial, você pode usar a porta adicional para a conexão heartbeat de série. À revelia, a primeira porta serial detectada no server CAM é configurada para o entrada/saída do console (para facilitar a instalação e outros tipos de acesso administrativo).

Se a máquina tem somente uma porta serial (COM1 ou ttyS0), você pode reconfigurar a porta

para servir como a Alta disponibilidade da conexão heartbeat. Isto é porque, depois que o software CAM é instalado, o console SSH ou KVM pode sempre ser usado para alcançar a interface da linha de comando do CAM.

Você pode permitir/desabilitação a porta serial com a caixa de verificação **de série do início de uma sessão do desabilitação nos** ajustes HA CAM (sob a **administração > Access Manager limpo > rede & Failover | Ajustes do Failover | Início de uma sessão de série do desabilitação**). Quando há somente uma porta serial na máquina CAM, esta caixa de verificação permite que os administradores desabilitem o início de uma sessão de série no COM1 de modo que possa ser usada como a interface serial da pulsação do coração para um par de gerentes HA-limpos do acesso.

Nota: O início de uma sessão de série **é permitido** à revelia no CAM. Se você usa o COM1 para a interface serial da pulsação do coração do CAM, você deve clicar a caixa de verificação **de série do início de uma sessão do desabilitação** para desabilitar o início de uma sessão de série no COM1.

Configurar o CAM HA-preliminar

Uma vez que você verificou as condições prévias, execute estas etapas para configurar o Access Manager limpo como o HA-preliminar para a Alta disponibilidade dos pares. Veja a figura para um exemplo da configuração de exemplo.

1. Abra o console do admin da Web para que o Access Manager limpo seja designado como o HA-preliminar, e vá à **administração > ao gerente CCA > ao certificado SSL** para configurar o certificado SSL para o CAM preliminar. O formulário **provisório do certificado da geração** aparece.**Nota:** As etapas de configuração HA neste documento supõem que um certificado provisório está exportado do CAM HA-preliminar para o CAM HA-secundário.*Se você usa um certificado provisório para os pares HA, execute estas etapas:*Termine o formulário **provisório do certificado da geração** e o clique **gerencie**. O certificado deve ser gerado para o Domain Name dos pares HA.Depois que você gerencie o certificado provisório, escolha a **chave/certificado da exportação CSR/Private da escolha um menu de ação**.Clique o botão da **exportação** para que a **chave privada atualmente instalada** exporte a chave privada SSL. Salvar o arquivo-chave ao disco. Você tem que importar esta chave no CAM HA-secundário mais tarde.Clique o botão da **exportação** para que o **certificado atualmente instalado** exporte o certificado atual SSL. Salvar o arquivo certificado ao disco. Você tem que importar este arquivo certificado no CAM HA-secundário mais tarde.*Se você usa um certificado assinado CA para os pares HA, execute estas etapas:***Nota:** O certificado assinado CA deve ser baseado no pode ser resolvido do Domain Name ao IP do serviço com o DNS. Consulte para controlar Certificados CAM SSL sob a seção da administração na ferramenta NAC de Cisco - a instalação e Guia de Administração CAM para mais informação.Escolha o **certificado de importação da escolha um menu de ação**.Use o **botão Browse** ao lado do campo do **arquivo certificado** e navegue ao certificado assinado CA.Choose CA-**assinou CERT X.509 PEM-codificado do** menu suspenso do **tipo de arquivo**.**Transferência de arquivo pela rede do** clique para importar o certificado. Note que você precisa de importar mais tarde este mesmo certificado no CAM HA-secundário.O clique **verifica e instala Certificados transferidos arquivos pela rede**.Escolha a **chave/certificado da exportação CSR/Private da escolha uma** lista de drop-down da **ação**.Clique o botão da **exportação** para que a **chave privada atualmente instalada** exporte a chave privada SSL associada com o certificado

assinado CA. Salvar o arquivo-chave ao disco. Você precisa de importar mais tarde este arquivo no CAM HA-secundário.

2. Vá à **administração > ao gerente CCA** e clique a aba da **rede & do Failover**. Escolha a opção HA-**preliminar do requisito de alta disponibilidade do** menu suspenso do **modo**. A Alta disponibilidade dos ajustes aparece.
3. Copie o valor do campo do **endereço IP de Um ou Mais Servidores Cisco ICM NT** sob **configurações de rede** e incorpore-o ao campo do **endereço IP de Um ou Mais Servidores Cisco ICM NT do serviço**. O endereço IP de Um ou Mais Servidores Cisco ICM NT das configurações de rede é o endereço IP de Um ou Mais Servidores Cisco ICM NT existente do Access Manager limpo atual. A ideia aqui é transformar este endereço IP de Um ou Mais Servidores Cisco ICM NT, que os servidores de acesso limpos já reconhecem, no endereço IP de Um ou Mais Servidores Cisco ICM NT virtual do serviço para os pares limpos do Access Manager.
4. Mude o endereço IP de Um ou Mais Servidores Cisco ICM NT sob **configurações de rede a um** endereço disponível, por exemplo, n.152.
5. Cada Access Manager limpo deve ter um nome de host original, tal como camanager1 e camanager2. Datilografe o nome de host do CAM HA-preliminar no campo de **nome de host** sob **configurações de rede**, e datilografe o nome de host do CAM HA-secundário no campo de **nome de host do par** sob **ajustes do Failover**.Um valor do **nome de host** é imperativo quando você estabelece a Alta disponibilidade, quando o **Domain Name do host** for opcional.Os campos do **nome de host** e de **nome de host do par** são diferenciando maiúsculas e minúsculas. Certifique-se combinar o que é datilografado aqui com o que é datilografado para o CAM HA-secundário mais tarde.
6. Do menu suspenso da **interface serial da pulsação do coração**, escolha a porta serial a que você conectou o cabo serial do CAM HA-preliminar, ou deixe este n/a se você não usa uma conexão serial.
7. Se sua máquina tem somente uma porta serial e você usa o COM1 como a interface serial da pulsação do coração, você deve verificar a caixa de verificação **de série do início de uma sessão do desabilitação** para assegurar-se de que o início de uma sessão de série esteja desabilitado no COM1. Veja a conexão serial para uns detalhes mais adicionais.
8. A fim manter a sincronização, o Access Manager limpo espreita dados de intercâmbio por uma rede do cruzamento. Você deve especificar um espaço de endereço de rede privada distribuído não atualmente em sua organização no **campo de rede do cruzamento**, tal como 10.10.10. A rede do cruzamento do padrão fornecida é 192.168.0.252. Se este os conflitos de endereço com sua rede, se certificam especificar um espaço de endereço privado diferente. Por exemplo, se sua organização usa a rede privada 192.168.151.0, uso 10.1.1.x como a rede do cruzamento. A máscara de sub-rede e o último octeto do endereço IP de Um ou Mais Servidores Cisco ICM NT são fixos, incorporam tão somente a porção de rede do endereço IP de Um ou Mais Servidores Cisco ICM NT ao **campo de rede do cruzamento**.
9. Clique a **atualização** e **recarregue-a** então para reiniciar o Access Manager limpo.Depois que o Access Manager limpo reinicia, certifique-se de que a máquina CAM funciona corretamente. Verifique para ver se os servidores de acesso limpos são conectados e os novos usuários estão autenticados.

Configurar o CAM HA-secundário

Execute estas etapas para configurar o CAM HA-secundário.

1. Abra o console do admin da Web para que o Access Manager limpo seja designado como o HA-secundário, e vá à **administração > ao gerente CCA > ao certificado SSL**.
2. Antes que você continue, execute estas etapas:Suporte a chave privada do CAM secundário.Certifique-se que a chave privada e os arquivos certificados SSL associados com o serviço IP/HA-Primary CAM estão disponíveis (exportado previamente como descrito em configurar o CAM HA-preliminar).
3. Importe o arquivo-chave privado e o certificado do CAM HA-preliminar como descrito:Na aba do **certificado SSL**, escolha o **certificado de importação da escolha um menu de ação**.O clique **consulta** ao lado do campo do **arquivo certificado**, e consulta a sua cópia de segurança do arquivo-chave privado gerado com o certificado que é usado para os pares HA.Escolha a **chave privada** como o tipo de arquivo.Clique a **transferência de arquivo pela rede** para transferir arquivos pela rede a chave privada.Com o **certificado de importação** escolhido da **escolha um menu de ação**, consulta ao certificado (provisório ou CA-assinado) que é associado com a chave privada.Choose CA-**assinou CERT X.509 PEM-codificado** como o tipo de arquivo.Clique a **transferência de arquivo pela rede** para transferir arquivos pela rede o certificado ou o certificado assinado CA provisório.O clique **verifica e instala Certificados transferidos arquivos pela rede**.Consulte para controlar Certificados CAM SSL sob a seção da administração na ferramenta NAC de Cisco - a instalação e Guia de Administração CAM para mais informação.
4. Vá à **administração > ao gerente > à rede & ao Failover CCA | As configurações de rede** e mudam o endereço IP de Um ou Mais Servidores Cisco ICM NT do CAM secundário a um endereço que seja diferente do endereço IP de Um ou Mais Servidores Cisco ICM NT HA-preliminar CAM e do endereço IP de Um ou Mais Servidores Cisco ICM NT do serviço.
5. Ajuste o valor do **nome de host** sob **configurações de rede ao** mesmo conjunto de valores para o **nome de host do par na** configuração HA-preliminar CAM. Veja a figura na seção preliminar HA.**Nota:** Os campos do **nome de host** e de **nome de host do par** são diferenciando maiúsculas e minúsculas. Certifique-se combinar o que é datilografado aqui com o que foi datilografado para o CAM HA-preliminar.
6. Escolha HA-**secundário no requisito de alta disponibilidade do** menu suspenso do **modo**. A Alta disponibilidade dos ajustes aparece.
7. Ajuste o valor do **endereço IP de Um ou Mais Servidores Cisco ICM NT do serviço** sob **ajustes do Failover ao** mesmo conjunto de valores para o **endereço IP de Um ou Mais Servidores Cisco ICM NT do serviço na** configuração HA-preliminar CAM.
8. Ajuste o valor do **nome de host do par** sob **ajustes do Failover ao** nome de host do CAM HA-preliminar.
9. Do menu suspenso da **interface serial da pulsação do coração**, escolha a porta serial a que você conectou o cabo serial do CAM HA-preliminar, ou deixe este n/a se você não usa uma conexão serial.
10. Se sua máquina tem somente uma porta serial e você usa o COM1 como a interface serial da pulsação do coração, você deve verificar a caixa de verificação **de série do início de uma sessão do desabilitação** para assegurar-se de que o início de uma sessão de série esteja desabilitado no COM1. Veja a conexão serial para uns detalhes mais adicionais.
11. Datilografe os mesmos ajustes da **interface de rede do cruzamento** que você tinha incorporado para o CAM HA-preliminar.
12. Clique a **atualização** e **recarregue-a** então.

Quando o CAM à espera começa acima, sincroniza automaticamente seu base de dados com o CAM ativo.

Finalmente, abra o console admin para o apoio outra vez e termine a configuração. Observe que o console admin para o apoio tem agora somente um módulo de gerenciamento.

Termine a configuração

Verifique os ajustes na página da **rede & do Failover** para o CAM à espera.

A configuração de alta disponibilidade está agora completa.

Falha sobre um par HA-CAM

aviso: A fim impedir toda a perda de dados possível dentro da sincronização de base de dados, certifique-se sempre de que o CAM à espera está vivo antes de falhar sobre o CAM ativo.

O Failover um pares HA-CAM, SSH à máquina ativa nos pares e executa um destes comandos:

- **parada programada** ou
- **repartição** ou
- **preste serviços de manutenção à parada do perfigo**Isto para todos os serviços na máquina ativa. Quando a pulsação do coração falha, a máquina à espera supõe o papel ativo. Execute o **começo do perfigo do serviço** para reiniciar serviços na máquina parada. Isto faz com que a máquina parada suponha o papel de standby.**Nota: o reinício do perfigo do serviço** não deve ser usado para testar a Alta disponibilidade (Failover). Em lugar de, Cisco recomenda a **parada programada** ou a **repartição na** máquina testar o Failover ou os comandos CLI, a **parada do perfigo do serviço** e o **começo do perfigo do serviço**.

Comandos CLI úteis para o HA

Estes são diretórios úteis a saber para o HA no CAM:

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

Este exemplo mostra que o lugar do HA debuga/arquivo de registro, assim como o nome de cada CAM (nó) nos 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
```

Como verificar status de tempo de corrida ativo/à espera no HA CAM

Este exemplo mostra como usar o CLI para determinar o status de tempo de corrida (ativo ou à espera) de cada CAM nos pares HA. Você pode geralmente encontrar o comando de **fostate.sh do** diretório de /store de sua última elevação, por exemplo, `/store/cca_upgrade-4.x.x.`

1. Execute o script de **fostate.sh no** primeiro 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. Execute o script de **fostate.sh no** 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
```

Como verificar Status de Configuração preliminar/secundário no HA CAM

Este exemplo mostra como usar o CLI para determinar o modo HA (preliminar/secundário) para qual cada CAM foi configurado inicialmente nos pares HA.

1. Encontre o nome dos CAM (Nós) com `/etc/ha.d/ha.cf`.
2. Verifique então o estado em cada CAM, por exemplo:
```
[root@cam1 ~]#
/perfigo/control/bin/check-ha cam1
active
[root@cam1 ~]# /perfigo/control/bin/check-ha cam2
active
```
3. Vai a `/perfigo/control/tomcat e executa o ls - o la`.Se os webapps apontam a **normal-webapps**, é o CAM preliminar.Se os webapps apontam ao **admin-webapps**, é o CAM secundário.Por exemplo, este CAM é o CAM preliminar:
```
[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 é o CAM secundário:
```
[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

Um erro ocorre em CAM **"SSKEY no server não combina o valor no base de dados"** quando CAS secundário em pares HA se torna ativo.

Solução

Resolva este problema quando você empurra manualmente CAS preliminar SSKEY para secundário (botão da restauração SSKEY, ou ultrapassagem manual no arquivo de /etc/.GUSSK em CAS). Geralmente, este problema ocorre quando você substitui um dispositivo e não faz delete/re-add ele desde/até o CAM. Neste caso, CAS tem seu próprio SSKEY baseado em seu MAC address e possivelmente não combina esse ajustado previamente no CAM. Isto é especialmente verdadeiro para CAS secundário porque tem um SSKEY baseado em seu próprio MAC address. Na configuração HA, mesmo secundária tem que usar CAS preliminar SSKEY baseado em CAS preliminar MAC.

Problema 2

Nos pares do Failover CAM, o CAM preliminar mostra o `AVISO! Conexões fechados a espreitar base de dados do [x.x.x.x] (endereço IP em standby)! Reinicie por favor o peer node para trazer bases de dados na sincronização!!` mensagem de erro.

Solução

Quando o link eth1 preliminar foi desligado e somente o enlace serial permanece, o CAM retorna um erro de base de dados que indique que não pode sincronização com suas contrapartes HA, e o administrador vê este erro no console de web CAM: .

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

Use Certificados auto-assinados ou da terceira nos pares CAM a fim resolver esta edição.

Problema 3

Como mudar o endereço IP de Um ou Mais Servidores Cisco ICM NT para a Alta disponibilidade no CAM

Solução

Tente derrubar o CAM secundário com **parada do perfigo do serviço**. Esta maneira, não dirige os serviços do perfigo, mas é ainda acessível pelo SSH. No CAM preliminar, mude o IP na **administração > no gerente > na rede CCA**. Não o deixe recarregar ainda. Vá então à aba do Failover, e mude o endereço IP de Um ou Mais Servidores Cisco ICM NT do serviço. Após esta etapa, recarregue-a então.

Uma vez que está inteiramente acima, certifique-se que é alcançável. Execute então o **começo do perfigo do serviço no** CAM secundário, e faça as mesmas mudanças que você fez ao preliminar. Então, recarregue-o, e deve vir acima como o secundário. Para o CERT SSL, se é emitido a um nome, a seguir mude a entrada de DNS de modo que o nome resolva ao IP novo do serviço. Se é emitido ao IP, regenere um certificado provisório novo. Neste momento, você quer provavelmente ter um início de uma sessão do usuário de teste. Se isso sucede, o Failover ao secundário, e certifica-se que você pode igualmente entrar.

Informações Relacionadas

- Página de suporte da ferramenta NAC de Cisco
- Suporte Técnico e Documentação - Cisco Systems