NAC-устройство (CCA): Настройка высокой доступности (HA) для Clean Access Manager (CAM)

Содержание

Введение

Этот документ описывает, как установить пару машин Clean Access Manager (CAM) для Высокой доступности (HA). Когда Чистые Access Manager развернуты в режиме Высокой доступности, можно гарантировать, что важный мониторинг, аутентификация и создание отчетов о задачах продолжаются в случае неожиданного завершения.

Примечание: См. раздел Высокой доступности (HA) Настройки устройства Cisco NAC - Установка чистого сервера доступа (CAS) и Руководство по администрированию, чтобы знать, как настроить функцию HA в CAS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на системе контроля доступа к сети Cisco NAC (NAC) Устройство - Версия 4.1 CAM.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Обзор

Эти ключевые точки предоставляют высокоуровневую сводку операции CAM HA:

1. Чистый режим Высокой доступности Access Manager является активной/пассивной двумя конфигурациями сервера, в которых резервная машина CAM действует как резервная копия к активной машине CAM.
2. Активный Чистый Access Manager выполняет все задачи для системы. Резервный CAM контролирует активный CAM и поддерживает, его база данных синхронизировалась с активной базой данных CAM.
3. Оба CAM совместно используют действительного Сервисного IP для интерфейса eth0, которому доверяют. Доменное имя должно использоваться для сертификата SSL.
4. Основные и вторичные машины CAM обмениваются тактовыми контрольными пакетами UDP каждые 2 секунды. Если таймер пульса истекает, перехват управления при отказе с синхронизацией состояния происходит.
5. Интерфейс eth1 и/или последовательный интерфейс на CAM могут использоваться для тактовых контрольных пакетов и синхронизации базы данных. Если и eth1 и последовательные интерфейсы настроены для биения, оба интерфейса должны быть не в состоянии для аварийного переключения происходить.

Чистый режим Высокой доступности Access Manager является активной/пассивной двумя конфигурациями сервера, в которых резерв Чистят действия машины Access Manager как резервную копию к активной Чистой машине Access Manager. В то время как активный CAM несет большую часть рабочей нагрузки под обычными условиями, резервные мониторы активный CAM и поддерживает, его хранилище данных синхронизировалось с данными активного CAM.

Если событие аварийного переключения происходит, такой, как будто активный CAM завершает работу или не отвечает на сигнал “биения” узла, резерв принимает роль активного CAM.

При первой настройке узлов HA необходимо задать Основной HA CAM и Вторичный HA CAM. Первоначально, Основным HA является активный CAM, и Вторичным HA является резервный (пассивный) CAM, но постоянно не назначены активное / пассивные роли. Если основной CAM выключается, вторичное устройство (резерв) становится активным CAM. Когда исходный основной CAM перезапускает, он принимает резервную роль.

Когда Чистый Access Manager запускает, это проверяет, чтобы видеть, активен ли его узел. В противном случае CAM, который запускает, принимает активную роль. Если узел активен, с другой стороны CAM, который запускается, становится резервом.

Можно настроить два Чистых Access Manager как пару HA в то же время, или можно добавить новый Чистый Access Manager к существующему автономному CAM для создания пары Высокой доступности. Для пары для появления к сети и Чистым Серверам доступа как один объект необходимо задать IP-адрес сервиса, который будет использоваться в качестве доверяемого интерфейса (eth0) адрес для пары HA.

Для создания перекрестной сети, в которой информацией о Высокой доступности обмениваются, вы подключаете порты eth1 обоих CAM и задаете адрес частной сети, не в настоящее время маршрутизировавшийся в вашей организации (по умолчанию HA перекрестно соединяют сеть, 192.168.0.252). Чистый Access Manager тогда создает частное, безопасное, с двумя узловыми сетями для портов eth1 каждого CAM, чтобы обмениваться трафиком биения UDP и синхронизировать базы данных. Обратите внимание на то, что CAM всегда использует eth1 в качестве интерфейса биения UDP.

Для дополнительной безопасности можно также подключить последовательные порты каждого Чистого Access Manager для обмена биения. В этом случае и биение UDP и последовательные интерфейсы биения должны быть не в состоянии для резервной системы вступать во владение.

Примечание: Для соединения кабеля последовательного порта для HA (или CAM HA или CAS HA), кабель последовательного порта должен быть кабелем “нуль-модема”.

Основные требования перед переходом

% Warning: Для предотвращения любой возможной потери данных в рамках синхронизации базы данных всегда удостоверяйтесь, что резервный (вторичный) Чистый Access Manager является оперативным прежде, чем переключиться при отказе активный (основной) Чистый Access Manager.

Прежде чем вы настроите Высокую доступность, гарантируете соответствие этим требованиям:

1. Вы получили Высокую доступность (Аварийное переключение) лицензия.**Примечание:** При установке Аварийного переключения CAM (HA) лицензия установите Лицензию на переключение к Основному CAM сначала, затем загрузите все другие лицензии. Автономные лицензии могут также использоваться для Высокой доступности.
2. Оба CAM установлены и настроены.

3. Для биения каждый CAM должен иметь уникальное имя хоста (или имя узла). Для пар CAM HA это имя хоста предоставлено узлу и должно быть решено через DNS или добавлено к/etc/hosts файлу узла.
4. У вас есть Сертификат подписанный ЦС для доменного имени пары CAM HA.
5. Основной HA CAM полностью настроен для операции во время выполнения. Это означает, что все заданы соединения с источниками аутентификационной информации, политикой, ролями пользователя, точками доступа, и так далее. Эта конфигурация автоматически дублирована во Вторичном HA (резервном) CAM.
6. Оба Чистых Access Manager доступны в сети (попытайтесь пропинговать их для тестирования соединения).
7. Машины, на которых установлено программное обеспечение CAM, имеют свободный Порт Ethernet (eth1) и по крайней мере один свободный последовательный порт. Используйте руководства спецификации для оборудования сервера для определения последовательного порта (ttyS0 или ttyS1) на каждой машине.
8. Во Внеполосных развертываниях Защита на уровне порта не включена на интерфейсах коммутатора, с которыми связаны CAS и CAM. Это может вмешаться в CAS HA и доставку DHCP.

Эти процедуры требуют, чтобы вы перезагрузили Чистый Access Manager. В то время его сервисы кратко недоступны. Настройте онлайновый CAM, когда время простоя окажет наименьшее количество влияния на ваших пользователей.

Примечание: Консоли веба - администратора Устройства Cisco NAC поддерживают Internet Explorer 6.0 или выше браузера.

Подключите чистые машины Access Manager

Существует два типа соединений между узлами CAM HA: один для обмена данными во время выполнения, которые касаются Чистых действий Access Manager и один для пульсирующего сигнала. В Высокой доступности Чистый Access Manager всегда использует интерфейс eth1 и для обмена данными и для обмена UDP биения. Когда пульсирующий сигнал UDP не в состоянии быть переданным и полученным в определенном периоде времени, резервная система вступает во владение. Для обеспечения дополнительных мер безопасности они настоятельно рекомендованы для добавления последовательного пульсирующего подключения между Чистыми узлами Access Manager. Последовательное подключение предоставляет дополнительный специализированный метод обмена биения, который должен отказать, прежде чем резервная система может вступить во владение. Обратите внимание на то, что соединение eth1 между узлами CAM является обязательным.

Физически соединитесь, узел Чистят Access Manager как показано:

- Используйте перекрестный кабель для соединения Портов Ethernet eth1 Чистых машин Access Manager. Это соединение используется для интерфейса UDP биения и обмена данными (зеркалирование базы данных) между узлами аварийного переключения.
- Используйте кабель последовательного порта нуль-модема для соединения (настоятельно рекомендованных) последовательных портов. Это соединение используется в качестве дополнительного биения последовательный обмен (поддержка активности) между узлами аварийного переключения.

Примечание: Для соединения кабеля последовательного порта для HA (или CAM HA или CAS HA), кабель последовательного порта должен быть кабелем “нуль-модема”.

Последовательное подключение

Если машина, которая выполняет программное обеспечение Clean Access Manager, имеет два последовательных порта, можно использовать дополнительный порт для последовательного пульсирующего подключения. По умолчанию первый последовательный порт, обнаруженный на сервере CAM, настроен для ввода с консоли / выходные данные (для упрощения установки и других типов административного доступа).

Если машина имеет только один последовательный порт (COM1 или ttyS0), можно реконфигурировать порт для служения в качестве пульсирующего подключения Высокой доступности. Это вызвано тем, что, после того, как программное обеспечение CAM установлено, SSH или консоль KVM могут всегда использоваться для доступа к интерфейсу командной строки CAM.

Вы можете позволить/запретить последовательный порт с флажком **Disable Serial Login** на параметрах настройки CAM HA (при **администрировании>, Чистят Access Manager> Сеть и Аварийное переключение |, Параметры настройки Аварийного переключения | Отключают Последовательный Вход в систему**). Когда существует только один последовательный порт на машине CAM, этот флажок позволяет администраторам отключать последовательный вход в систему на COM1 так, чтобы это могло использоваться в качестве Последовательного интерфейса Биения для пары Чистых HA Access Manager.

Примечание: Последовательный вход в систему **включен** по умолчанию на CAM. При использовании COM1 для Последовательного интерфейса Биения CAM необходимо нажать флажок **Disable Serial Login** для отключения последовательного входа в систему на COM1.

Настройте основной HA CAM

Как только вы проверили предварительные условия, выполните эти шаги для настройки Чистого Access Manager как Основного HA для пары Высокой доступности. Посмотрите рисунок для примера примера конфигурации.

1. Откройте консоль веба - администратора для Чистого Access Manager, чтобы определяться как Основное HA, и перейдите **к администрированию> Менеджер CCA> сертификат SSL** для настройки сертификата SSL для основного CAM. **Генерировать** форма **Временного сертификата** появляется.**Примечание:** Действия настройки HA в этом документе предполагают, что временный сертификат экспортируется от Основного HA CAM до Вторичного HA CAM.*При использовании временный сертификат для пары HA, выполняете эти шаги*:Заполните **Генерировать** форму **Временного сертификата** и нажмите **Generate**. Сертификат должен генерироваться для доменного имени пары HA.После того, как вы генерируете временный сертификат, выбираете **Export CSR / CSR/Private Key/Certificate** от **Выбирания меню Действие**.Нажмите кнопку **Export** для **В настоящее время Устанавливаемого Секретного ключа** для экспортирования секретного ключа SSL. Сохраните контрольный файл на диск. Необходимо импортировать этот ключ во Вторичный HA CAM позже.Нажмите кнопку **Export** для **В настоящее время Устанавливаемого Сертификата** для экспортирования текущего сертификата SSL. Сохраните файл сертификата на диск. Необходимо импортировать этот файл сертификата во Вторичный HA CAM позже.*При использовании Сертификат подписанный ЦС для пары HA, выполняете эти шаги:***Примечание:** Сертификат подписанный ЦС должен основываться на доменном

имени, разрешимом к Сервисному IP через DNS. См. Управляют сертификатами SSL CAM под разделом администрирования в устройстве Cisco NAC - Установка CAM и Руководство по администрированию для получения дополнительной информации.Выберите **Import Certificate** из **Выбирания меню Действие**.Используйте **Кнопку обзора** рядом с полем **Certificate File** и перейдите к Сертификату подписанный ЦС.Выберите **CA-signed PEM-encoded X.509 Cert** из раскрывающегося меню **Типа файла**.Нажмите **Upload** для импорта сертификата. Обратите внимание на то, что необходимо импортировать этот тот же сертификат во Вторичный HA CAM позже.Нажмите **Verify и Install Uploaded Certificates**.Выберите **Export CSR / CSR/Private Key/Certificate** от **Выбирания** выпадающего списка **действия**.Нажмите кнопку **Export** для **В настоящее время Устанавливаемого Секретного ключа** для экспортирования секретного ключа SSL, привязанного к Сертификату подписанный ЦС. Сохраните контрольный файл на диск. Необходимо импортировать этот файл во Вторичный HA CAM позже.
2. Перейдите **к администрированию> Менеджер CCA** и нажмите вкладку **Network & Failover**. Выберите опцию **HA-Primary** из раскрывающегося меню **Режима Высокой доступности**. Параметры настройки Высокой доступности появляются.
3. Копируйте значение от **поля IP Address** при **Настройках сети** и введите его в поле **Service IP Address**. IP-адресом Настроек сети является существующий IP-адрес текущего Чистого Access Manager. Идея здесь состоит в том, чтобы повернуть этот IP-адрес, который Чистые Серверы доступа уже распознают в действительный IP-адрес сервиса для Чистой пары Access Manager.
4. Измените IP-адрес при **Настройках сети** к доступному адресу, например, n.152.
5. У каждого Чистого Access Manager должно быть название уникального узла, такое как camanager1 и camanager2. Введите имя хоста Основного HA CAM в поле **Host Name** при **Настройках сети** и введите имя хоста Вторичного HA CAM в поле **Peer Host Name** при **Параметрах настройки Аварийного переключения**.Значение **Имени хоста** является обязательным, когда вы устанавливаете Высокую доступность, в то время как **Доменное имя Хоста** является дополнительным.Поля **Host Name и Peer Host Name** учитывают регистр. Удостоверьтесь, что совпали с тем, что введено здесь с тем, что введено для Вторичного HA CAM позже.
6. От раскрывающегося меню **Последовательного интерфейса Биения** выберите последовательный порт, с которым вы подключили кабель последовательного порта Основного HA CAM, или оставьте это н/д, если вы не используете последовательное подключение.
7. Если ваша машина только имеет один последовательный порт, и вы используете COM1 в качестве Последовательного интерфейса Биения, необходимо проверить флажок **Disable Serial Login**, чтобы гарантировать, что последовательный вход в систему отключен на COM1. Посмотрите Последовательное подключение для получения дальнейшей информации.
8. Для поддержания синхронизации Чистый Access Manager взаимодействует с обменом данными перекрестной сетью. Необходимо задать пространство адреса частной сети, не в настоящее время маршрутизировавшееся в организации в **Перекрестном Поле сети**, такой как 10.10.10. Перекрестная предоставленная сеть по умолчанию 192.168.0.252. Если это конфликты адресов с вашей сетью, удостоверьтесь, что задали другое частное пространство адресов. Например, если ваша организация использует частную сеть 192.168.151.0, используйте 10.1.1.x в качестве перекрестной сети. Маска подсети и последний октет IP-адреса исправлены, поэтому только вводят часть сети

IP-адреса в **Перекрестном Поле сети**.

9. Нажмите **Update** и затем **Перезагрузку** для перезапуска Чистого Access Manager.После Чистых перезапусков Access Manager удостоверьтесь, что машина CAM работает должным образом. Проверьте, чтобы видеть, связаны ли Чистые Серверы доступа, и новые пользователи аутентифицируются.

Настройте вторичный HA CAM

Выполните эти шаги для настройки Вторичного HA CAM.

1. Откройте консоль веба - администратора для Чистого Access Manager, чтобы определяться как Вторичное HA, и перейдите **к администрированию> Менеджер CCA> сертификат SSL**.
2. Прежде чем вы продолжитесь, выполните эти шаги:Резервное копирование секретный ключ вторичного CAM.Удостоверьтесь, что файлы и сертификата SSL с закрытым ключом, привязанные к Сервисному CAM IP/HA-Primary, доступны (ранее экспортируемый, как описано в, Настраивают Основной HA CAM).
3. Импортируйте файл закрытого ключа и сертификат Основного HA CAM, как описано:Во вкладке **сертификата SSL** выберите **Import Certificate** из **Выбирания меню Действие**.Нажмите **Browse** рядом с полем **Certificate File** и перейдите к своей резервной копии файла закрытого ключа, генерируемого с сертификатом, который используется для пары HA.Выберите **Private Key** в качестве типа файла.Нажмите **Upload** для загрузки секретного ключа.С **Сертификатом импорта**, выбранным из **Выбирания меню Действие**, перейдите к сертификату (или временный или подписанный CA), который привязан к секретному ключу.Выберите **CA-signed PEM-encoded X.509 Cert** в качестве типа файла.Нажмите **Upload** для загрузки временного сертификата или Сертификата подписанный ЦС.Нажмите **Verify и Install Uploaded Certificates**.См. Управляют сертификатами SSL CAM под разделом администрирования в устройстве Cisco NAC - Установка CAM и Руководство по администрированию для получения дополнительной информации.
4. Перейдите **к администрированию> Менеджер CCA> Сеть и Аварийное переключение | Настройки сети** и измените IP-адрес вторичного CAM к адресу, который отличается от Основного HA IP-адреса CAM и IP-адреса сервиса.
5. Установите значение **Имени хоста** при **Настройках сети** к тому же заданному значению для **Одноранговое Имени хоста** в Основной HA конфигурации CAM. Посмотрите рисунок в HA Основной раздел.**Примечание:** Поля **Host Name и Peer Host Name** учитывают регистр. Удостоверьтесь, что совпали с тем, что введено здесь с тем, что было введено для Основного HA CAM.
6. Выберите **HA-Secondary** в раскрывающемся меню **Режима Высокой доступности**. Параметры настройки Высокой доступности появляются.
7. Установите значение **IP-адреса сервиса** при **Параметрах настройки Аварийного переключения** к тому же заданному значению для **IP-адреса сервиса** в Основной HA конфигурации CAM.
8. Установите **Одноранговое** значение **Имени хоста** при **Параметрах настройки Аварийного переключения** к имени хоста Основного HA CAM.
9. От раскрывающегося меню **Последовательного интерфейса Биения** выберите последовательный порт, с которым вы подключили кабель последовательного порта

Основного HA CAM, или оставьте это н/д, если вы не используете последовательное подключение.

10. Если ваша машина только имеет один последовательный порт, и вы используете COM1 в качестве Последовательного интерфейса Биения, необходимо проверить флажок **Disable Serial Login**, чтобы гарантировать, что последовательный вход в систему отключен на COM1. Посмотрите Последовательное подключение для получения дальнейшей информации.
11. Введите те же **Перекрестные** параметры настройки **Сетевого интерфейса**, как вы ввели для Основного HA CAM.
12. Нажмите **Update** и затем **Перезагрузку**.

Когда резервный CAM запускает, он автоматически синхронизирует свою базу данных с активным CAM.

Наконец, откройте консоль администрирования для резерва снова и завершите конфигурацию. Заметьте, что консоль администрирования для резерва теперь имеет только один модуль управления.

Завершите конфигурацию

Проверьте параметры настройки на странице **Network & Failover** для резервного CAM.

Конфигурация высокой доступности теперь завершена.

Переключаясь при отказе пара CAM HA

% Warning: Для предотвращения любой возможной потери данных в рамках синхронизации базы данных всегда удостоверяйтесь, что резервный CAM является оперативным прежде, чем переключиться при отказе активный CAM.

Чтобы к аварийному переключению пара CAM HA, SSH к активной машине в паре и выполняют одну из этих команд:

- **завершение** или
- **перезагрузка** или
- **сервисный perfigo останавливается**Это останавливает все сервисы на активной машине. Когда биение отказывает, резервная машина принимает активную роль. Выполните **сервисный perfigo начинают** перезапускать сервисы на остановленной машине. Это заставляет остановленную машину принимать роль резерва (standby).**Примечание: сервисный перезапуск perfigo** не должен использоваться для тестирования Высокой доступности (аварийное переключение). Вместо этого Cisco рекомендует **завершению** или **перезагрузке** на машине протестировать аварийное переключение, или команды CLI, **сервисный perfigo останавливается**, и **сервисный perfigo запускаются**.

Полезные команды CLI для HA

Это полезные каталоги для знания для HA на CAM:

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

Данный пример показывает местоположение отладки/файлов журнала HA, а также название каждого CAM (узел) в паре 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
```

Как Проверить Активный/Резервный Статус времени выполнения на CAM HA

Данный пример показывает, как использовать CLI для определения статуса времени выполнения (активный или резервный) каждого CAM в паре HA. Можно обычно находить **команду fostate.sh** из каталога хранилища / последнего обновления, например, `/store/cca_upgrade-4.x.x.`

1. Выполните сценарий **fostate.sh** на первом 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. Выполните сценарий **fostate.sh** на втором 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*

Как Проверить Основной/Вторичный Статус конфигурации на CAM HA

Данный пример показывает, как использовать CLI для определения режима HA (Основного/Вторичного), для которого каждый CAM был первоначально настроен в паре HA.

1. Найдите название CAM (узлы) с `/etc/ha.d/ha.cf.`
2. Затем проверьте статус на каждом CAM, например:`[root@cam1  ~]# /perfigo/control/bin/check-ha  cam1`
   `active`
   `[root@cam1  ~]#  /perfigo/control/bin/check-ha  cam2`
   `active`
3. Перейдите `/perfigo/control/tomcat and perform ls -la.`Если webapps указывает к **обычному-webapps**, это - основной CAM.Если webapps указывает **admin-webapps**, это - вторичный CAM.Например, этот CAM является основным CAM:`[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` Этот CAM является вторичным CAM:`[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
```

Устранение неполадок

Проблема 1

Ошибка происходит на CAM **"SSKEY на сервере, не совпадает со значением в базе данных"**, когда вторичный CAS в паре HA становится активным.

Решение

Решите эту проблему при ручном продвижении основного SSKEY CAS к вторичному (кнопка SSKEY сброса или ручная замена на/etc/.GUSSK файле на CAS). Обычно, эта проблема происходит, когда вы заменяете устройство и делаете не delete/re-add это от/к CAM. В этом случае CAS имеет свой собственный SSKEY на основе его MAC-адреса и возможно не совпадает с тем, ранее установленным на CAM. Это особенно истинно для вторичного CAS, потому что он имеет SSKEY на основе своего собственного MAC-адреса. На конфигурации HA даже вторичная должна использовать основной SSKEY CAS на основе основного MAC CAS.

Проблема 2

В паре CAM Аварийного переключения основной CAM показывает `WARNING! Closed connections to peer [x.x.x.x](standby IP Address) database! Please restart peer node to bring databases in sync!!` error message.

Решение

Когда основная ссылка eth1 была разъединена, и только последовательное соединение остается, CAM возвращает ошибку базы данных, которая указывает, что это не может синхронизировать с ее дубликатом HA, и администратор видит эту ошибку в вебе - консоли CAM:.

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

Используйте самоподписанный или сторонние сертификаты на паре CAM для решения этого вопроса.

Проблема 3

Как изменить IP-адрес для Высокой доступности на CAM

Решение

Попытка перевести вторичный CAM в нерабочее состояние с **сервисным perfigo останавливается**. Таким образом, это не выполняет сервисы perfigo, но это все еще доступно SSH. На основном CAM измените IP в **администрировании> Менеджер CCA> Сеть**. Еще не позволяйте ему перезагрузка. Затем перейдите к вкладке Failover и измените IP-

адрес сервиса. После этого шага затем перезагрузите его.

Как только это подключено полностью, удостоверьтесь, что это достижимо. Затем работайте**, сервисный perfigo запускаются** на вторичном CAM и вносят те же изменения, как вы сделали к основному. Затем перезагрузите его, и это должно подойти как вторичное устройство. Для свидетельства SSL, если это выполнено к названию, затем изменяют Запись DNS так, чтобы название решило к новому сервисному IP. Если это выполнено к IP, восстановите новый временный сертификат. На этом этапе вы, вероятно, хотите сделать, чтобы вошел тестовый пользователь. Если это успешно выполняется, аварийное переключение к вторичному устройству, и удостоверьтесь, что вы также в состоянии войти.

Дополнительные сведения

- Страница технической поддержки устройства Cisco NAC
- Cisco Systems – техническая поддержка и документация