

Как решить окончные точки копии Главного обеспечения совместной работы (РСА) Cisco

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Проблема](#)

[Решение](#)

[Доступ к корневому каталогу](#)

Введение

Этот документ описывает, как Решить Cisco Главные Оконечные точки Копии Обеспечения Совместной работы.

Внесенный Джозефом Коглином, специалистом службы технической поддержки Cisco

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание Модуля Материально-технических ресурсов и это - операции в Главном Обеспечении
- Основные основные принципы Linux относительно Главного Обеспечения

Этот документ требует, чтобы была внедрена эта конфигурация:

- Если у вас не будет доступа к корневому каталогу см. Нижний Раздел Под названием Доступ к корневому каталогу, полный Доступ к корневому каталогу будет необходим -
- Главное приложение Обеспечения установлено, и вы копировали окончные точки в Системе Материально-технических ресурсов.напр. Две окончных точки с тем же названием: SEPAA11BB22CC33

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Главный интерфейс командной строки обеспечения
- Главные материально-технические ресурсы Обеспечения Модуль
- Все применимые версии программного обеспечения
- Никакие требования к оборудованию не требуются

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были

запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды

Проблема

Cisco главное обеспечение - двойные телефоны

Этот документ для сред, которые копируют телефоны в системе или сценариях, где удалять и повторно добавляет окончательных точек, применимо.

Этот процесс демонтирует все телефоны, и после этого процесс повторно добавляет их назад

Решение

Шаг 1. Войдите в PCA через Secure Shell (SSH) как root и порт 26

Шаг 2. Ввод. `CD/opt/emms/emsam/bin/`

Шаг 3. Теперь вы остановите сервисы с Вводом `./cpcmcontrol.sh` останавливаются

Шаг 4. . Вы теперь проверите , чтобы гарантировать, что все сервисы не работают
Вводом. `статус./cpcmcontrol.sh`

- Как только все сервисы не работают, переходят к следующему шагу

Шаг 5. . Вы теперь запустите только сервис Базы данных Вводом. `./start_db.sh`

Шаг 6 и Шаг 7 удалят телефоны из Базы данных В шаге 11, вы возвратите их в систему

Шаг 6. Ввод. `./refreshCDT.sh` (ждут, пока он не завершает),

Шаг 7. Ввод. `./refreshPhone.sh` (ждут, пока он не завершает),

Шаг 8. Теперь вы принесете резервное копирование сервисов с
Вводом. `перезапуск./cpcmcontrol.sh`

(выполните `./cpcmcontrol.sh статус` периодически, чтобы гарантировать, что все сервисы возвращаются),

Шаг 9. Когда gui возвращается, входят как globaladmin пользователь и делают кластерное обнаружение данных как следующий шаг.

Шаг 10. Затем вы выполните Кластерное обнаружение данных: **Материально-технические ресурсы Navigateto> список Материально-технических ресурсов> Кластерное обнаружение данных.**

Шаг 11. Выберите **Run теперь** (Этот шаг получит назад телефоны),

Шаг 12. Ждите, пока это не закончено, и телефоны должны вернуться и не иметь никаких копий.

Примечание: Это обнаружение зависит от количества конечных точек в вашем кластере, и время к завершению может варьироваться

Например, цели можно сравнить запуск и время окончания и видеть эту деталь, которую одно единственное заняло 38 секунд для завершения.

The screenshot shows the Cisco Prime Collaboration Assurance interface. At the top, there is a navigation bar with the Cisco logo and the text 'Prime Collaboration Assurance'. Below this, there is a breadcrumb trail: 'Home / Inventory / Inventory Schedule'. There are three tabs: 'IP Phone Inventory Schedule', 'IP Phone XML Inventory Schedule', and 'Cluster Data Discovery Schedule', with the third tab being active. The main heading is 'Cluster Data Discovery Schedule'. Underneath, there is a section titled 'Cluster Device Discovery Status' with the following information: 'Discovery Status Discovery completed', 'Last Discovery Start Time 07-Sep-2017 12:00:00 AM EDT', and 'Last Discovery End Time 07-Sep-2017 12:00:38 AM EDT'. Below this is another section titled 'Cluster Device Discovery Schedule' with the text: 'The following schedule is configured and is active. To apply your changes, select Apply when you have finished any operations.' There are two dropdown menus for 'Hour' and 'Minute', both set to '0'. At the bottom of this section are two buttons: 'Apply' and 'Run Now'.

Примечание: Для получения информации PCA получит телефоны через Сервис поступающая в реальном времени данные (RIS) и Административный Расширяемый язык разметки гипертекста (XML) (AXL) от Издателя Менеджера связи Cisco Unified (CUCM)

Полезные журналы, если встречаются с какими-либо проблемами:

Если вы все еще встречаетесь с копиями см. журналы, упомянутые для рассмотрения

Примечание: Если вы не будете иметь см. Доступ к корневому каталогу раздела, полный Доступ к корневому каталогу будет необходим. Как только полному доступу к корневому каталогу включают, используйте программу, такую как Winscp, чтобы подключить и использовать порт 26 и учетные данные пользователя маршрута.

/opt/emms/cuom/log/CUOM/CDT

RISCollection.log, CDT.log, CDTAPI.log, CDTAudit.log

/opt/emms/emsam/log/Inventory/CDT.log

/opt/emms/emsam/log/Tomcat/CDT.log

/var/log/refreshPhone.log <-это сообщит , были ли какие-либо проблемы с выполнением сценариев

Дальнейшие примечания по устранению проблем и Общие сведения:

Можно также хотеть видеть, можно ли перезапустить сервис RIS в кластере Call Manager, поскольку это может разрешить некоторые несоответствия или проблемы.

Когда телефоны будут собраны в сист, он будет использовать axl+ris, поэтому если у вас будут проблемы, можно хотеть перезапустить сервис RIS в сист.

Не будет никакого воздействия на бизнес при перезапуске сервиса RIS в кластере тогда как перезапуск сервиса AXL не рекомендуется во время рабочих часов.

Дополнительно редко будет необходимо перезапустить сервис AXL поэтому прежде, чем сделать так, я обратился бы к журналам, чтобы видеть, необходим ли перезапуск.

Также гарантируйте, что Call Manager управляют, и в сист под System> Server сист имя хоста/ip издателя является отвечающим на команду ping и разрешимым.

Поскольку можно столкнуться со случаем, где вы обнаружили и управляли Call Manager как ip, однако в System> Server Call Managers это перечислено именем хоста.

То, что происходит, - когда PCA соберет телефоны через axl+ris, это перечислит, однако, это перечислено под System> Server поэтому, если вам перечислят его как имя хоста, и это не разрешимо rca тогда, то вы никогда не будете получать эти телефоны, даже если сист будут управлять, потому что этим управлял ip.

Этот сценарий исправлен двумя путями:

Сценарий 1

Шаг 1. Вход в систему в PCA через пользователя маршрута SSH и порт 26

Шаг 2. CD / и т.д.

Шаг 3. Хосты Вай

Шаг 4. . потребуйте i вставки

- Вставленный как пример (существует пространство промежуточный ip и имя хоста),
- В данном примере 10.10.10.10 и testexample.csc.edu используется.

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1          localhost.localdomain localhost
::1              localhost6.localdomain6 localhost6
172.20.116.24    cm90assu
10.10.10.10      testexample.csc.edu
```

Шаг 5. . Откройте вновь свой Call Manager впоследствии. Перейдите к: Материально-технические ресурсы> Управление запасами> Инфраструктура> Приложения UC> Communications Server

Сценарий 2

Шаг 1. Гарантируйте, что обратный просмотр Сервиса имен Domain (DNS) разрешим через dns для устройства, на которое влияют.

Шаг 2. Откройте вновь Кластер Call Manager. Перейдите к: **Материально-технические**

- Выберите Call Managers, на которые влияют, и выберите Rediscover

Доступ к корневому каталогу

В этом разделе описывается получить полный Доступ к корневому каталогу для PCA

Шаг 1. Войдите через SSH к PCA и используйте порт 26 в качестве пользователя Admin

Шаг 2. Ввод. **root_enable**

Введите в пароле при загрузке, который вы хотите

Шаг 3. Ввод. **root** и тип в пароле при загрузке

Шаг 4. . После авторизации как корневой Ввод./opt/emms/emsam/bin/enableRoot.sh

Шаг 5. . Ввод. **passwd** и повторно вводит в вашем пароле при загрузке

Теперь необходимо быть в состоянии закрыть Сеанс SSH и повторно войти непосредственно как root