Настройте Устройство записи в Мосту Вызова CMS/Acano

Содержание

Введение

Этот документ описывает действия настройки, должен был установить Устройство записи на Мосту вызова (CB) Cisco, встречающей сервер (CMS).

The Recorder доступен от выпуска 1.9 сервера Acano. The Recorder предоставляет capabilility записи совещаний и сохранения записей на хранении документов Протокола NFS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

1. CMS 1.9 или выше

2. Почтальон от Google Chrome

3. Программный интерфейс приложения CMS (API)

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, используемые в здесь запущенном с конфигураций по умолчанию. Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

Общие сведения

1. The Recorder ведет себя как Расширяемый Протокол Обмена сообщениями и Присутствия (XMPP) клиент, таким образом, сервер XMPP должен быть включен на сервере, который размещает Мост Вызова.

2. Лицензия устройства записи, которая должна быть на CB а не сервере устройства записи, если рабочие версии до CMS 2. X, дополнительные сведения здесь https://kb.acano.com/content/23/280/en/how-does-licensing-work-on-the-acano-solution.html.

3. Каталог протокола NFS, который может быть настройкой на Windows Server или Linux.

Для Windows Server выполните действия в этой ссылке: https://technet.microsoft.com/en-us/library/jj574143 (v=ws.11) .aspx.

Для Linux выполните действия в этой ссылке: https://help.ubuntu.com/lts/serverguide/network-file-system.html.

Примечание: Для NFS, который работает на Windows Server 2008 R2 там заплата для проблемы разрешений: https://support.microsoft.com/en-us/kb/2485529.

Развертывания

Поддерживаемые развертывания

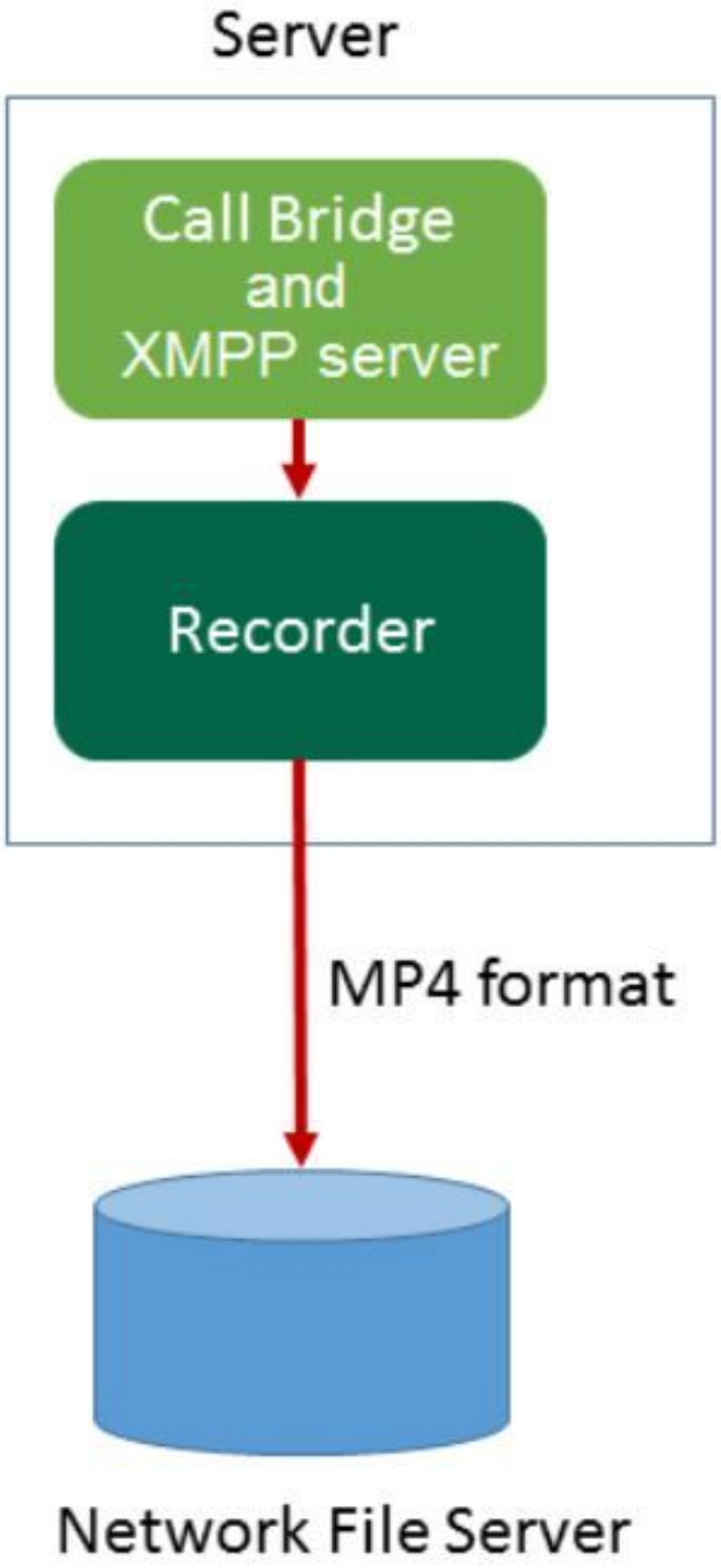
1. The Recorder должен быть размещен на сервере Acano, который удален к серверу, который размещает CB как показано на этом рисунке:

2. Избыточные развертывания Устройства записи также поддерживаются. Если резервирование является настройкой, записи с балансировкой нагрузки между всеми регистрирующими устройствами (серверы). Это означает, что каждый CB будет использовать каждое доступное Устройство записи, поскольку эти данные показывают:

3. Когда существует множественный CBS, то же применяется в противоположном. Весь CBS будет использовать Устройство записи availabe для них, поскольку эти данные показывают:

Другая настройка

The Recorder может также быть размещен на том же сервере как CB, но это должно только использоваться для тестирования или очень небольших развертываний, посмотрите рисунок. Недостаток здесь - то, что можно только быть в состоянии сделать 1 - 2 одновременных записей:


Server
Call Bridge and XMPP server
Recorder
MP4 format
Network File Server

Настройка

Часть 1: На сервере Устройства записи:

o. Настройте Устройство записи для прослушивания на интерфейсе (интерфейсах) по Вашему выбору с этой командой:

устройство записи слушает <интерфейс [: порт] белый список>

b. Если устройство записи находится на локальном CB, интерфейс должен быть набором к “loopback”, так используйте эту команду:

устройство записи слушает lo:8443

c . Если это должно слушать на определенном интерфейсе, скажем, то используйте это:

устройство записи слушает a:8443

Примечание: При настройке устройства записи на узле кластеризованного CB интерфейс должен быть локальным интерфейсом прослушивания узла, на котором настраивается устройство записи.

---

d. Заставьте файл сертификата использоваться устройством записи. Можно использовать сертификат, который уже существует и файл закрытого ключа, используемый CB, например.

устройство записи certs <файл ключей> <certificatefile>

e. Добавьте сертификат CB к базе доверенных сертификатов Устройства записи с помощью команды:

доверие устройства записи <crt-связка-(-bundle-)>

Crt-связка-(-bundle-) должна содержать сертификат, используемый CB, если другой. Если в кластере, это должно содержать сертификаты каждого CB в кластере.

_____ F. Задайте имя хоста или IP-адрес NFS и каталог на NFS для Хранения записей:

nfs устройства записи <имя хоста/IP>: <каталог>

Примечание: The Recorder не аутентифицируется на NFS, но важно, чтобы Сервер Устройства записи имел доступ для чтения-записи к каталогу NFS.

---

g. Включите Устройство записи с использованием команды:

устройство записи включает

Часть 2: на CB:

Создайте пользователя API на CB, это требуется для дальнейших конфигураций с помощью API-функции:

Создайте пользователя с этими шагами:

o. Подключение через Secure Shell (SSH) или консоль к CB с использованием учетных данных admin.

b. Пользователь добавляет api **<username>**, затем нажимает **Клавишу Return** и вводит пароль, придерживавшийся **Клавишей Return** .

Часть 3: Использование API:

1. Загрузка и Почтальон Установки
от; https://chrome.google.com/webstore/detail/postman/fhbjgbiflinjbdggehcddcbncdddomop?hl=en

2. Введите URL доступа API в строку адреса, например:

https://<Callbridge_IP>:445/api/v1 / <объект>

Затем установленный на аутентификации, имени пользователя и пароле от Части 2, в соответствии с Авторизацией с **Основной Аутентификацией** как тип:

Примечание: Это предполагает, что в настоящее время нет никакого устройства записи или callProfile, настроенного на CB. В противном случае можно модифицировать устройство записи, которое существует и/или callProfile с использованием метода PUT.

---

3. Добавьте устройство записи к CB с API:

o. Передайте пустой POST с https://<Callbridge_IP>:445/api/v1/recorders

b. Передайте GET с тем же URL в (a), скопируйте ID устройства записи без кавычек к Блокноту

c . Установите URL устройства записи путем передачи PUT
с https://<Callbridge_IP>:445/api/v1/recorders / <recorderid> и добавьте это в BODY перед выполнением PUT:

url=https://127.0.0.1:8443 (если устройство записи находится на локальном CB),

или

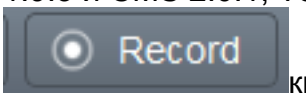
url=https://Адрес <IP устройства записи>:8443 (если устройство записи не находится на

локальном CB),

Пример:

Примечание: ***dtmfProfile***, ***callProfile*** и ***callLegProfile*** особенно важны для оконечных точек SIP, которые присоединяются **к cospace** конференции. Они позволяют Оконечной точке быть в состоянии запустить/остановить запись к/ота вызова **cospace**.

Как от CMA 1.9.3 и CMS 2.0.1, Тоны DTMF не требуются теперь

существует 

кнопка, это добавлено к клиенту, когда устройство записи присутствует на или известный callbridge, с которым связан клиент.

4. Создайте callProfile:

o. Передайте пустой POST с https://<Callbridge_IP>:445/api/v1/callProfiles

b. Передайте GET с тем же URL в (a), скопируйте callProfile ID без кавычек к Блокноту

c . Установите recordingMode на callProfile путем передачи PUT с https://<Callbridge_IP>:445/api/v1/callProfiles / <ID профиля вызова> и добавьте в BODY перед выполнением PUT.

recordingMode=Manual (если вы хотите, чтобы абоненты начали делать запись записей DTMF использования),

или

recordingMode=Automatic (если запись должна запуститься автоматически, когда вызовы запущены),

Пример:

Примечание: При использовании POSTER из Firefox необходимо щелкнуть по “content to send”, тогда выбирают "body from parameters"

прежде, чем передать PUT/POST, этот способ, которым это скомпилировано в коде (кодах), который может понять CB.

---

5. Добавьте профиль вызова к Системным профилям:

callProfile определяет, могут ли вызовы быть записями и если они могут быть сделаны с или без вмешательства пользователя.

Передайте PUT с https://<Callbridge_IP>:445/api/v1/system/profiles после добавления callProfile в BODY

callProfile = <ID профиля вызова>

Пример:

Если recordingMode установлен в Руководство, необходимо заставить профиль DTMF определять, как пользователи могут запустить и остановить записи с помощью Тонов DTMF.

6. Создайте профиль DTMF:

o. Передайте Пост с https://<Callbridge_IP>:445/api/v1/dtmfProfiles после установки startRecording = ** 7 и stopRecording = ** 8 (например), в BODY как startRecording = ** 7&stopRecording = ** 8.

Пример:

b. Передайте GET, чтобы видеть новый профиль DTMF, затем скопировать ID без кавычек к блокноту.

7. Создайте профиль CallLeg:

CallLegProfiles определяет поведение incall. В этом случае это определяет, могут ли быть зарегистрированы вызовы.
Создайте профиль ветви вызовов следующим образом:

o. Передайте Пост с https://<Callbridge_IP>:445/api/v1/CallLegProfiles после добавления recordingControlAllowed=true в BODY:

Пример:

b. Примените CallLegProfile путем передачи PUT с https://<Callbridge_IP>:445/api/v1/system/profiles и добавления callLegProfile = <callLegProfile_ID> в BODY:

Пример:

8. Примените профиль DTMF:

Передайте PUT с https://<Callbridge_IP>:445/api/v1/system/profiles после добавления dtmfProfile в BODY dtmfProfile = <dfmt ID Профиля>

Пример:

Проверка и устранение неполадок

1. После того, как настроенный, проверьте его статус с этими командами, это должно быть подобно этим выходным данным:

устройство записи

Локальный автономный CB:

```
acanosrv01> recorder
Enabled                 : true
Interface whitelist     : lo:8443
Key file                : callbridgecert.key
Certificate file        : callbridgecert.cer
Trust bundle            : callbridgecert.cer
NFS domain name         : 10.48.36.246
NFS directory           : /acano
```

Или если кластеризованный CB:

```
acanosrv05> recorder
Enabled                 : true
Interface whitelist     : a:8443
Key file                : forallcert05.key
Certificate file        : forallcert05.cer
Trust bundle            : TrustBundle.crt
NFS domain name         : 10.48.36.246
NFS directory           : /cluster-alero-aca-recordings
```

2. Передайте GET для просмотра системного профиля, необходимо видеть callProfile, CallLegProfile и dtmfProfile в результате с:

https://<Callbridge_IP>:445/api/v1/system/profiles

Пример:

3. Для проверки, что было настроено на CallProfile используйте это на API:

https://<Callbridge_IP>:445/api/v1/callProfiles / <callProfile_ID>

Это показывает, что методы записи были установлены, или Автоматические или Ручные, как показано:

4. Для проверки, что настроено на CallLegProfile используйте этот API:

https://<Callbridge_IP>:445/api/v1/callLegProfiles / <callLegProfile_ID>

Пример выходных данных:

5. Для проверки, что было настроено на Профиле DTMF используйте это на API:

https://<Callbridge_IP>:445/api/v1/dtmfProfiles / <dtmfProfile_ID>

Это показывает, что методы записи были установлены, или Автоматические или Ручные, как показано:

Примечание: Профили DTMF не работают в вызовах "точка-точка", таким образом, можно только использовать ручную запись в пространстве.

---

6. Для отображения, что зарегистрировано относительно устройства записи, выполняет команду:

системный журнал придерживается

Необходимо видеть что-то подобное этим выходным данным:

20 июня прокси устройства записи 20:38:49 kern.info acanosrv05 [1]: Соединение 20:38:49 20.06.2016 от 10.48.54.75:39439:

Аутентификация успешно выполнилась
20 июня прокси устройства записи 20:38:49 kern.info acanosrv05 [1]: Соединение 20:38:49 20.06.2016 от 10.48.54.75:39439:

Соединение завершилось
20 июня прокси устройства записи 20:38:53 kern.info acanosrv05 [1]: Соединение 20:38:53 20.06.2016 от 10.48.54.76:35141:

Аутентификация успешно выполнилась
20 июня прокси устройства записи 20:38:53 kern.info acanosrv05 [1]: Соединение 20:38:53 20.06.2016 от 10.48.54.76:35141:

Соединение завершилось

В данном примере acanosrv05 является сервером, размещающим устройство записи, и другие узлы CB, соединяющиеся с ним, 10.48.54.75 и 10.48.54.76.

Этот показ, который удаленный CB правильно подключает и аутентифицирует с Устройством записи.

Если бы устройство записи локально для CB, то соединение прибыло бы из петлевого IP:

20 июня прокси устройства записи 20:40:52 kern.info acanosrv01 [1]: Соединение 20:40:52 20.06.2016 от 127.0.0.1:45380:

Аутентификация успешно выполнилась
20 июня прокси устройства записи 20:40:52 kern.info acanosrv01 [1]: Соединение 20:40:52 20.06.2016 от 127.0.0.1:45380:

Соединение завершилось

Примечание: Большинство журналов, отнесенных к процессам устройства записи, показывают в системном журнале как **прокси устройства записи**, они дают индикацию, где могло бы отказывать устройство записи.

Другие системные журналы показывают следующим образом для устройства записи:

В этом случае регистрирующее устройство найдено, и запись запускается автоматически:

"20 июня регистрирующее устройство user.info acanosrv02 host:server: .info: 21:16:19 1: доступный (1 записи)"

Если сбои записи тогда проверяют, найдено ли регистрирующее устройство:

"20 июня 21:16:19 user.info acanosrv02 host:server: .info: никакое найденное регистрирующее

устройство".

Если вы видите такое предупреждение, проверьте сертификат в доверии устройства записи, чтобы гарантировать, что это - корректное, используемое CB.

Проверьте системный журнал, чтобы видеть, установлено ли хранилище NFS:

Если хранилище NFS не будет установлено, то вы будете видеть "Подведенный для установки хранилища NFS".

Проверьте, что папка NFS и набор на устройстве записи server:/Folder-name совпадают с тем, что настроено на хранилище NFS.

Выполните API для проверки сигналов тревоги, которые касаются устройства записи:

https://<callBridge_IP> api/v1/система/сигналы тревоги

Если существует недостаточное пространство на диске, необходимо видеть "recorderLowDiskSpace".

Затем проверьте, что хранилище NFS, на которое ссылается устройство записи, имеет достаточно дискового пространства.