Configurazione del registratore in CMS/Acano Call Bridge

Sommario

Introduzione

Questo documento descrive la configurazione necessaria per configurare il registratore sul componente Call Bridge (CB) di un Cisco Meeting Server (CMS).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CMS 1.9 o superiore
- Postman da Google Chrome
- API (Application Program Interface) CMS

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

Il registratore CMS è disponibile dalla versione 1.9 del server CMS (ex Acano). Il registratore consente di registrare le riunioni e di salvare le registrazioni su un supporto di archiviazione NFS (Network File System).

Il registratore si comporta come un client XMPP (Extensible Messaging and Presence Protocol), pertanto il server XMPP deve essere abilitato sul server che ospita il bridge di chiamate.

La licenza di registrazione è necessaria e deve essere applicata al componente CallBridge e non al server di registrazione.

La directory NFS (Network File System) è necessaria e può essere configurata su Windows Server o Linux.

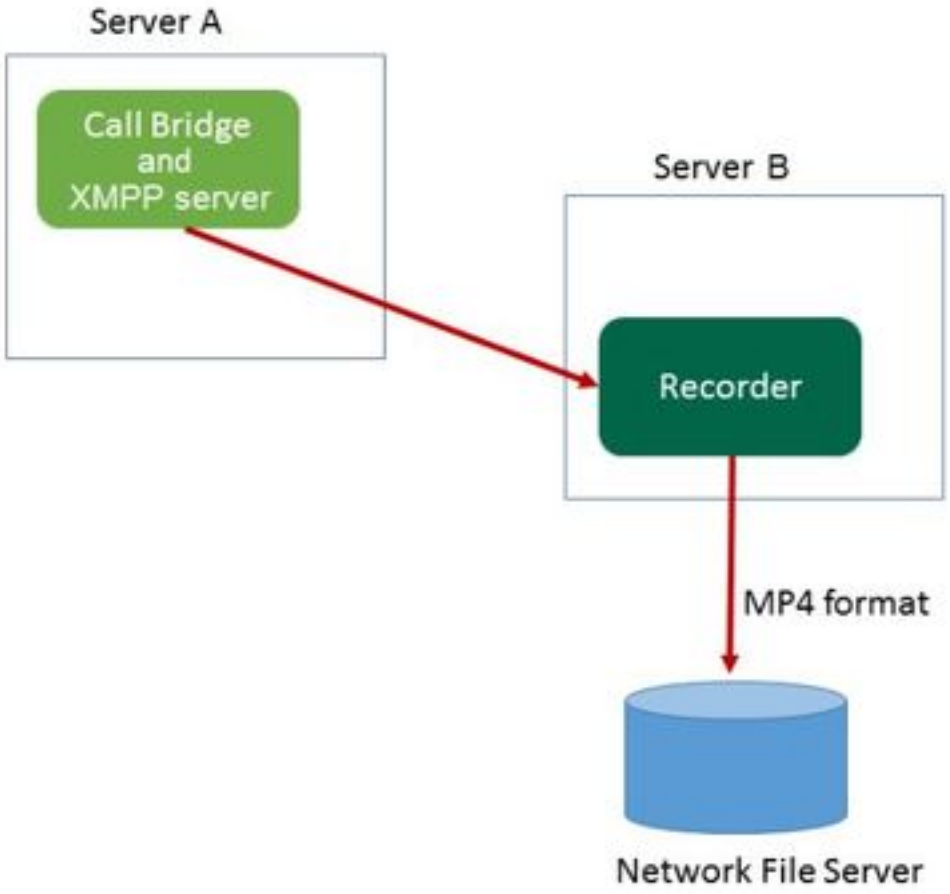
- Per il server Windows, eseguire la procedura per distribuire il file system di rete in Windows
- Per Linux, seguire i passaggi per distribuire Network File System su Linux

  Nota: Per NFS eseguito in Windows Server 2008 R2 è disponibile un hotfix per il problema di autorizzazione.

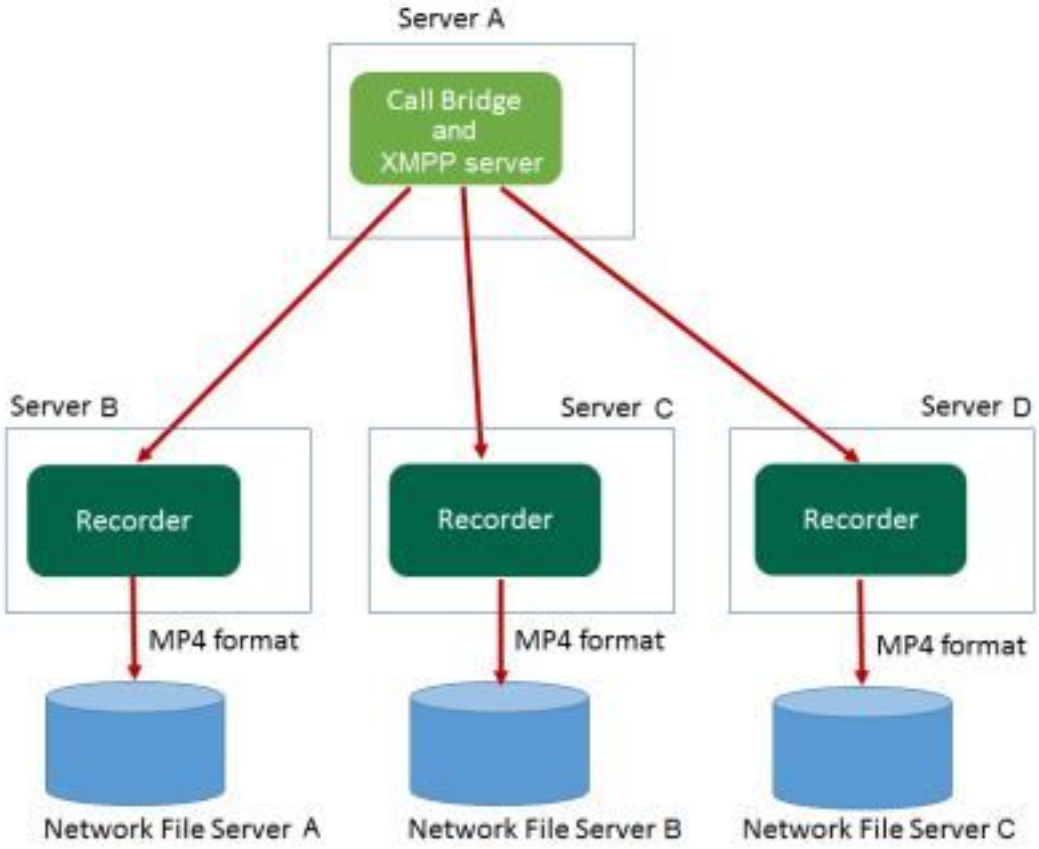
Distribuzioni

Distribuzioni supportate

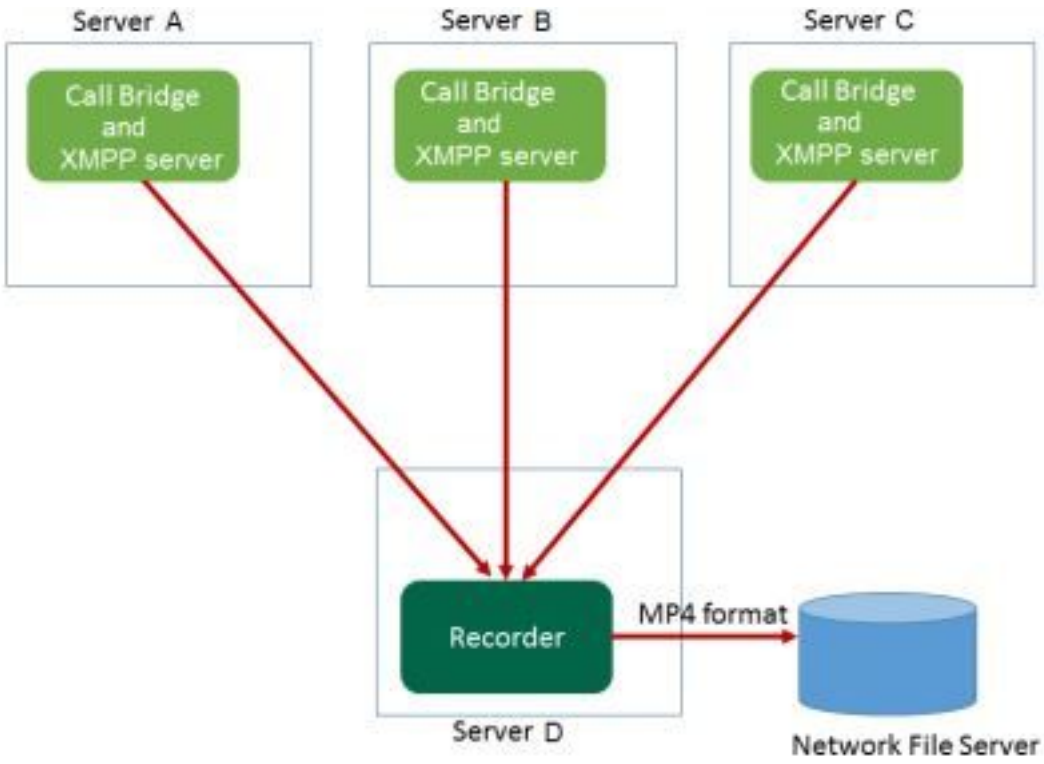
1. Il registratore deve trovarsi su un server CMS/Acano remoto rispetto al server che ospita la BC, come mostrato in questa immagine



2. È inoltre supportata l'installazione ridondante del registratore. Se è impostata la ridondanza, le registrazioni vengono bilanciate in base al carico tra tutti i dispositivi di registrazione (server). Ciò significa che ogni CB utilizza ogni registratore disponibile, come mostrato in questa immagine

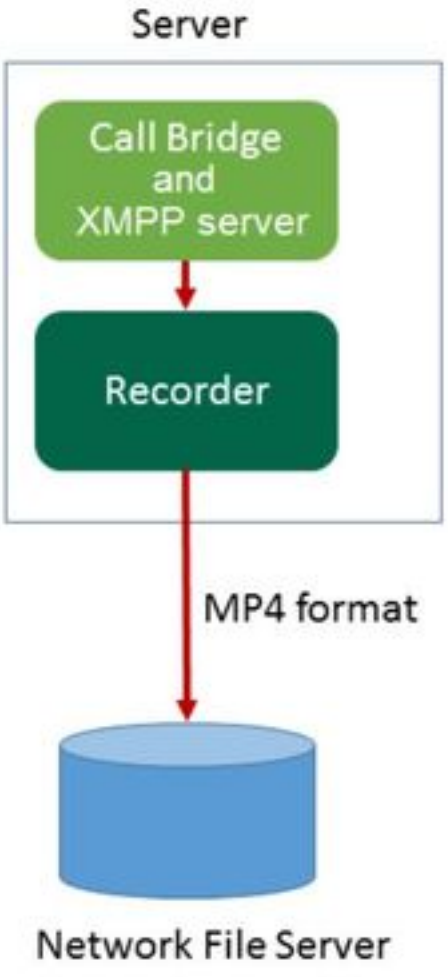


3. Lo stesso principio si applica nell'opposto, quando vi sono più BC. Tutti i nodi CB utilizzano il registratore disponibile, come mostrato in questa immagine



Altre impostazioni

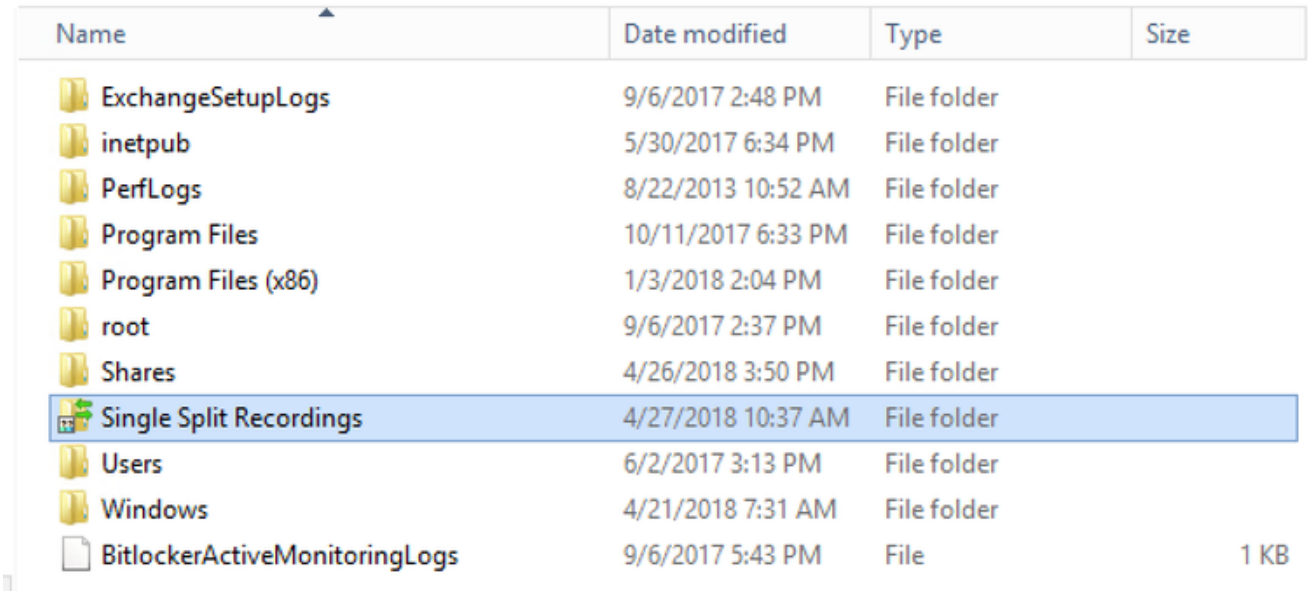
Il registratore può anche essere ospitato sullo stesso server del CB, ma deve essere utilizzato solo per test o installazioni di dimensioni molto ridotte. Vedere l'immagine successiva per riferimento. Lo svantaggio è che è possibile eseguire solo 1-2 registrazioni simultanee:



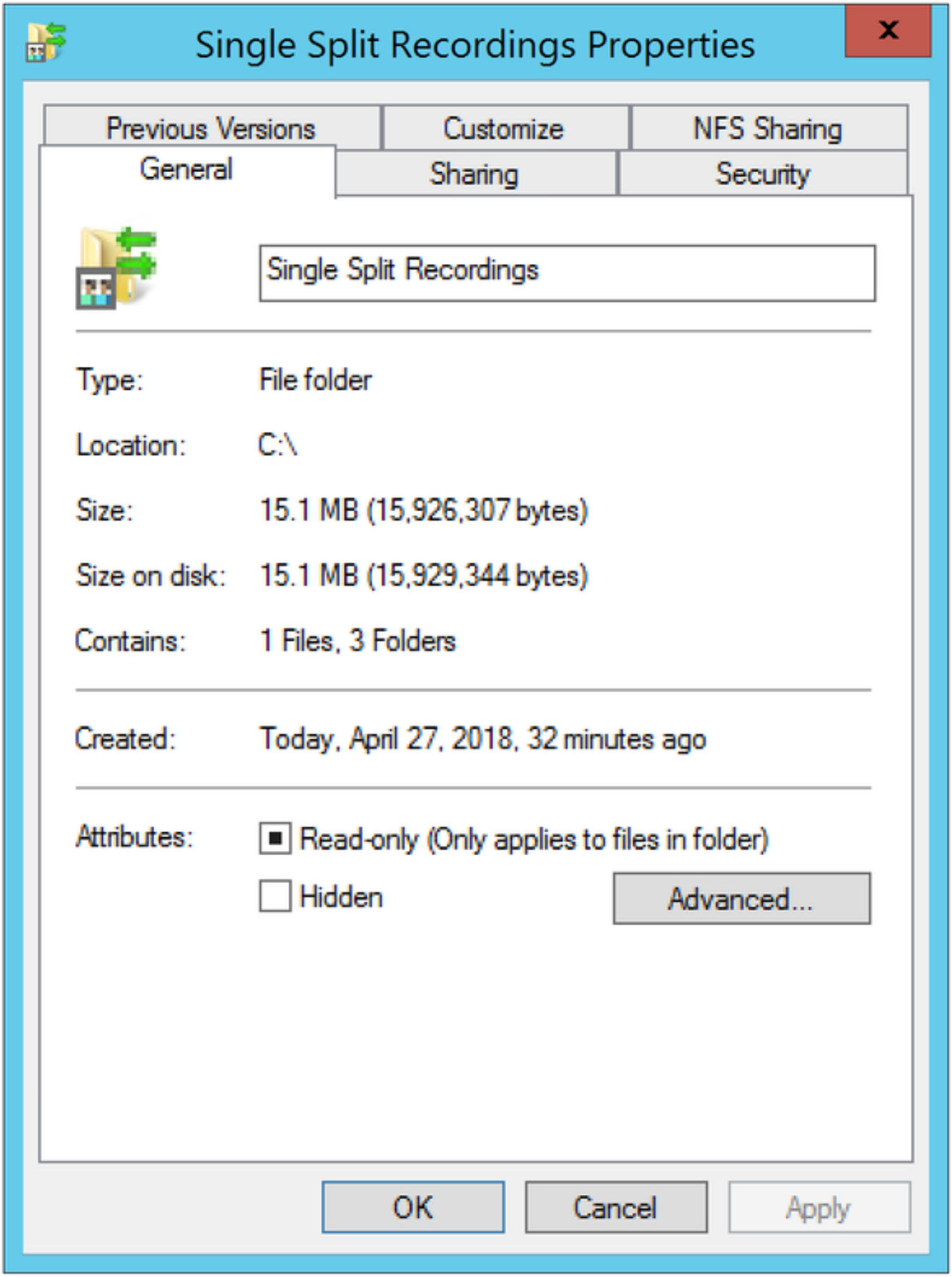
Configurazione

Passaggio 1. Configurare una cartella di condivisione NFS in un server Windows

r. In Esplora risorse creare una nuova cartella per la condivisione NFS. In questo esempio è stata creata una cartella denominata **Single Split Recordings** sul disco locale



b. Fare clic con il pulsante destro del mouse sulla cartella e selezionare **Proprietà**



c. Selezionare la scheda **Condivisione NFS** in alto a destra. La cartella viene visualizzata come **Non condivisa**. In questo esempio la cartella è stata condivisa in precedenza. In caso contrario, sarà necessario visualizzare un percorso di rete vuoto e la cartella verrà visualizzata come **Non condivisa**

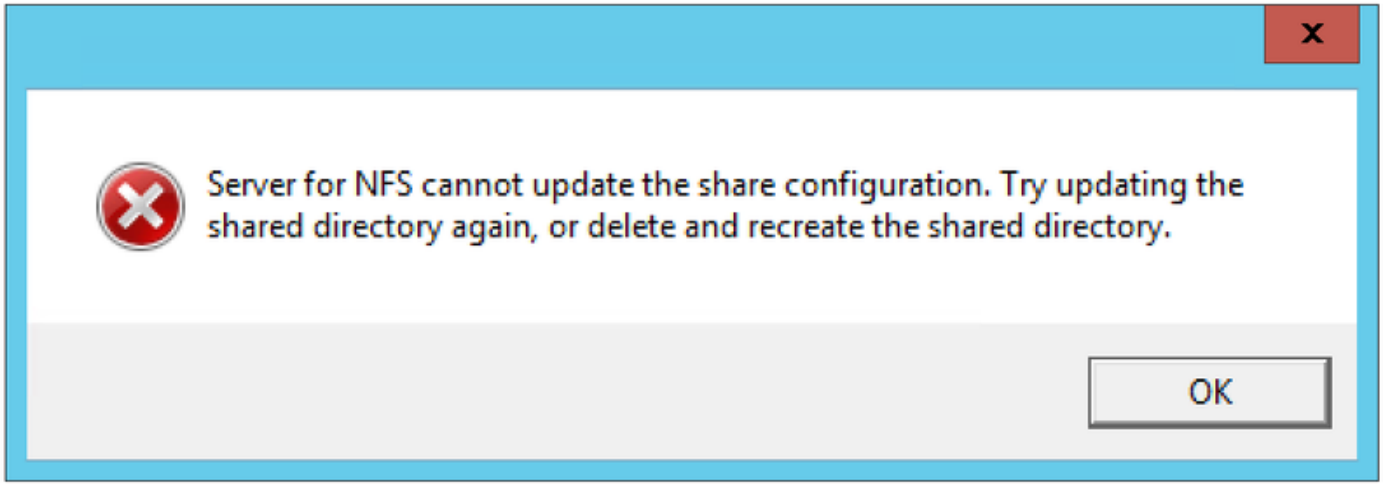
d. Seleziona **Gestisci condivisione NFS**

e. Selezionare la casella di controllo accanto a **Condividi questa cartella**

f. Immettere il nome della cartella condivisa in **Nome condivisione** senza spazi

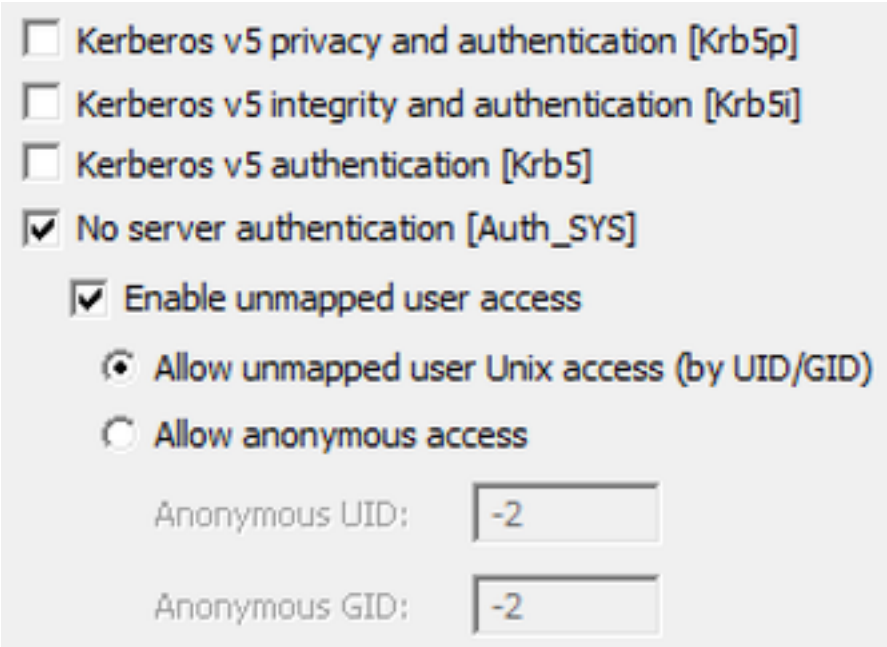
Nota: Viene utilizzato dai client NFS e dal registratore CMS per trovare questa cartella.

Nota: Verificare che il nome della condivisione di cartella non contenga spazi. In caso affermativo, non sarà possibile salvare le modifiche e verrà visualizzata la seguente finestra di errore:



g. Mantenere la codifica predefinita **ANSI** valore

h. Per impostazione predefinita, tutte le caselle di controllo di autenticazione sono contrassegnate. Deselezionare tutte le caselle **Kerberos** opzioni di autenticazione lasciando solo **Nessuna autenticazione server [Auth_SYS]**



i. Seleziona **Consenti accesso Unix utente non mappato (tramite UID/GID)**

j. In basso, selezionare **Autorizzazioni** per impostare le autorizzazioni sulla condivisione di rete

Nota: L'impostazione predefinita è Sola lettura per tutti i computer. Il registratore deve disporre dell'accesso in lettura/scrittura, in modo da poter modificare l'impostazione predefinita per **TUTTI I COMPUTER** o aggiungere regole specifiche per il registratore. La procedura ottimale consiste nel disabilitare l'accesso a TUTTI I COMPUTER modificandolo in **Nessun accesso** e aggiungendo nuove autorizzazioni per l'indirizzo IP dei server che devono accedere alla condivisione.

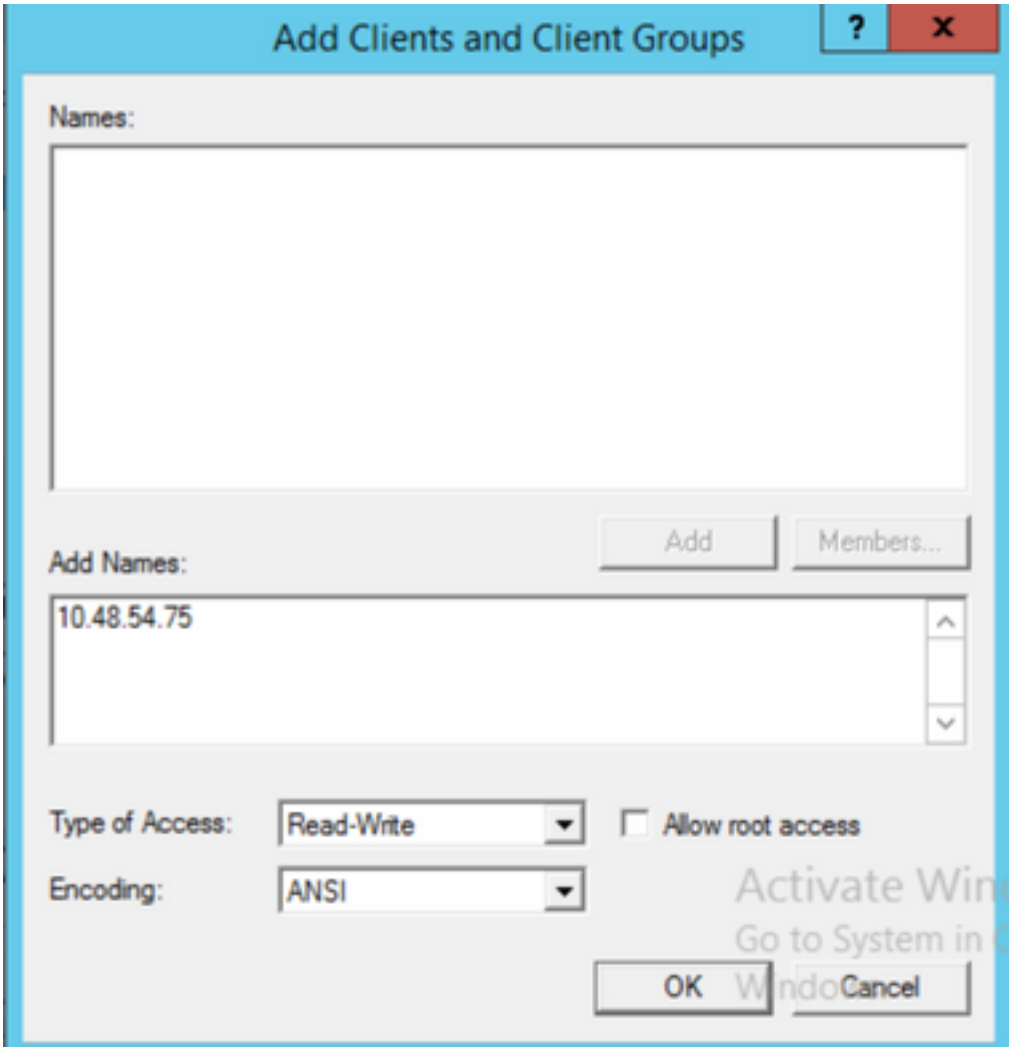
k. Per aggiungere le autorizzazioni per il registratore, selezionare **Aggiungi**

l. Dentro **Aggiungi nomi**, immettere l'indirizzo IP del server di registrazione. Nell'esempio, il server di registrazione è 10.48.54.75

m Seleziona **Read-Write** accesso

n. Lascia codifica come **ANSI**

o. Esci **Consenti accesso alla radice** disattivato



p. Selezionare **OK** per chiudere la finestra di dialogo delle autorizzazioni

d. Seleziona **TUTTI I COMPUTER**

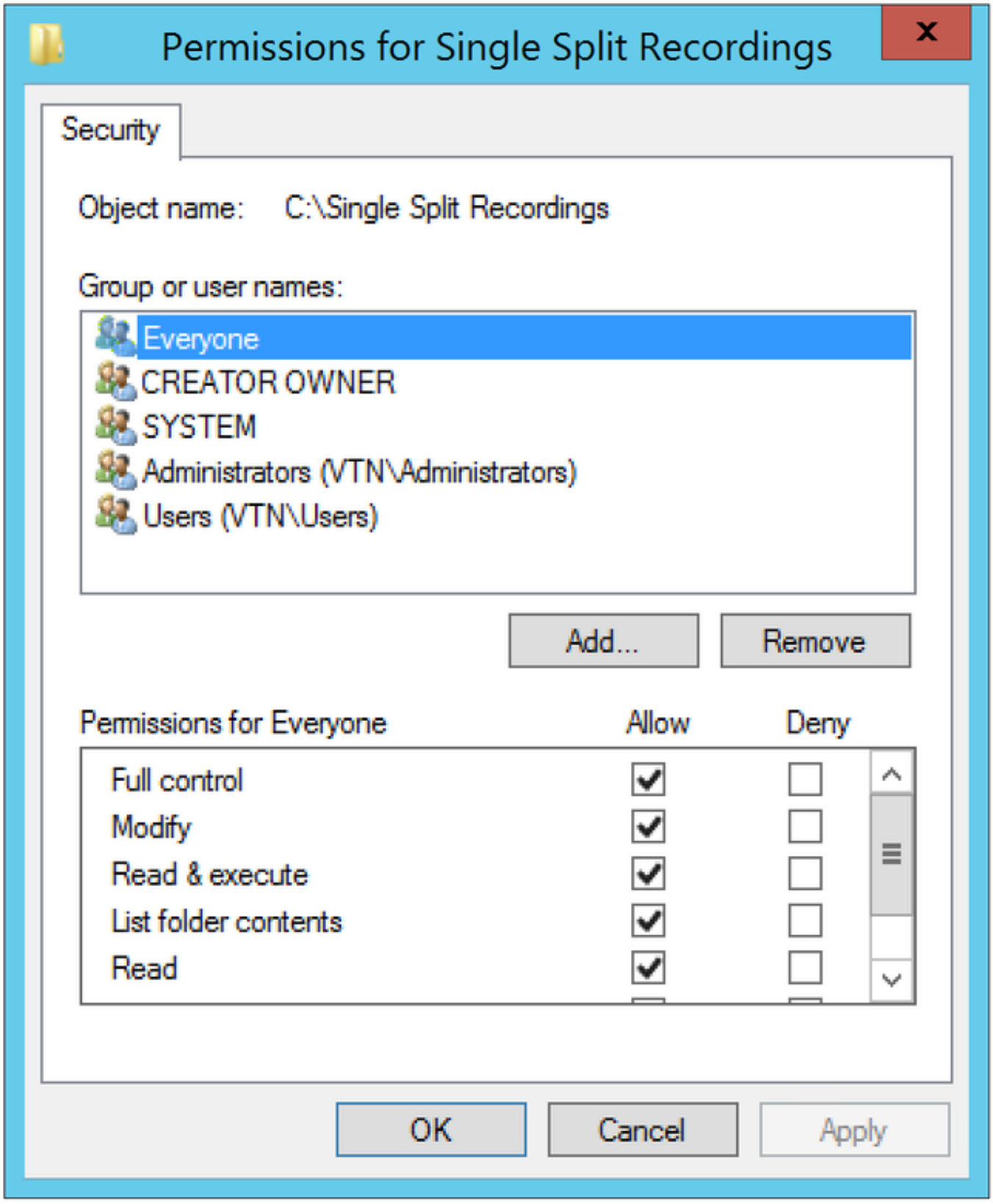
r. Cambia **Tipo di accesso** a **Nessun accesso**

s. Seleziona **OK** per chiudere la finestra autorizzazioni

t. Seleziona **OK** per tornare alla finestra Proprietà cartella

u. Seleziona **Sicurezza**

> **Nota:** Il gruppo **Everyone** deve disporre dell'accesso completo alla cartella. Se non è presente nell'elenco, selezionare **Modifica** per aprire l'editor delle autorizzazioni. Selezionare **Aggiungi** per aggiungere un utente e nel campo Nomi immettere **Everyone** e selezionare OK. Selezionare **Everyone** nell'elenco, selezionare la casella di controllo **Full control** (Controllo completo) e scegliere **OK**. Selezionare nuovamente **OK** per chiudere le proprietà. Se configurato correttamente, assomiglia all'immagine successiva:



Passaggio 2. Configurare e abilitare il registratore sul server di registrazione

r. Configurare il registratore per l'ascolto sulle interfacce desiderate con questo comando:

ascolto registratore <interface[:port] whitelist>

b. Se il registratore si trova sul CB locale, l'interfaccia deve essere impostata su "loopback", quindi utilizzare questo comando:

log ascolto registratore:8443

c. Se deve ascoltare su un'interfaccia specifica, diciamo "a", allora usa questo:

ascolto da registratore a:8443

> **Nota:** Se si configura il registratore su un nodo di CB in cluster, l'interfaccia deve essere l'interfaccia di ascolto locale del nodo su cui viene configurato il registratore.

d. Impostare il file del certificato che deve essere utilizzato dal registratore. È possibile, ad esempio, utilizzare un certificato già esistente e un file di chiave privata utilizzato dal CB.

recorder certs <file chiave> <file certificato>

e. Aggiungere il certificato CB all'archivio di attendibilità del registratore utilizzando il comando:

trust registratore <crt-bundle>

Il crt-bundle deve contenere il certificato utilizzato dalla BC, se diverso. Se si trova in un cluster, deve contenere i certificati di tutte le CA del cluster.

f. Specificare il nome host o l'indirizzo IP del NFS e la directory sul NFS in cui memorizzare le registrazioni:

recorder nfs <nome host/IP>:<directory>

> **Nota:** Il registratore non esegue l'autenticazione all'NFS, ma è importante che il server di registrazione disponga dell'accesso in lettura/scrittura alla directory NFS.

g. Abilitare il registratore con il comando:

attivazione registratore

Passaggio 3. Creazione di un utente API sul CB

Creare un utente API sul CB. Questa operazione è necessaria per ulteriori configurazioni che utilizzano la funzione API:

Creare l'utente eseguendo la procedura seguente:

r. Connettersi al server CB tramite SSH (Secure Shell) o console con le credenziali di amministratore.

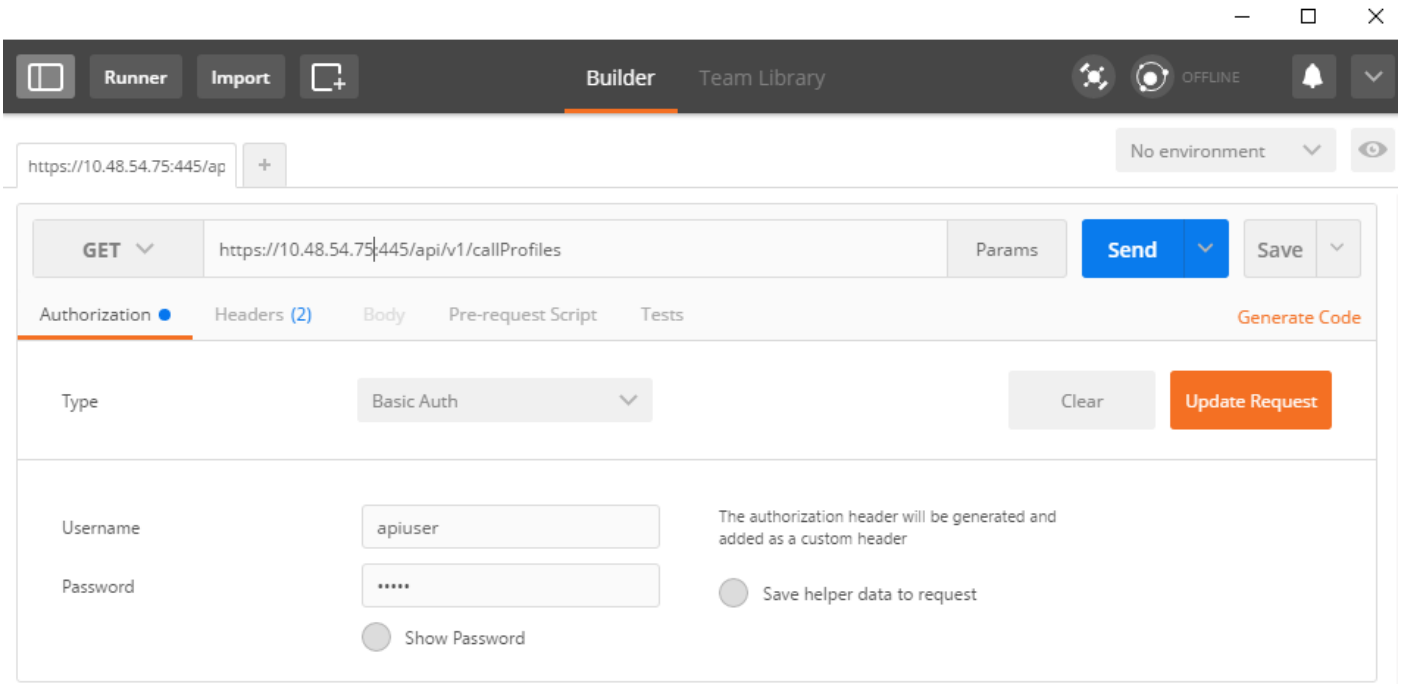
b. L'utente aggiunge l'api **<username>**, quindi preme il tasto **Invio** e immette la password seguita

dal tasto **Invio**.

Passaggio 4. Aggiungere il registratore al CB utilizzando l'API

1. Scarica e installa Postman da qui

2. Inserire l'URL di accesso API nella barra degli indirizzi, ad esempio: **https://<Callbridge_IP>:445/api/v1/<entità>**. Quindi, impostare in autenticazione, il nome utente e la password dal passaggio 3, in Autorizzazione con **autenticazione di base** come tipo



> **Nota:** Ciò presuppone che non vi sia attualmente alcun registratore o profilo di chiamata configurato sul CB. In caso contrario, è possibile modificare un registratore esistente e/o chiamare Profilo utilizzando il metodo PUT.

3. Aggiungere il registratore al CB con l'API

r. Inviare un POST vuoto con https://<Callbridge_IP>:445/api/v1/recorders

b. Inviare un GET con lo stesso URL in (a), copiare l'ID del registratore, senza virgolette, nel Blocco note

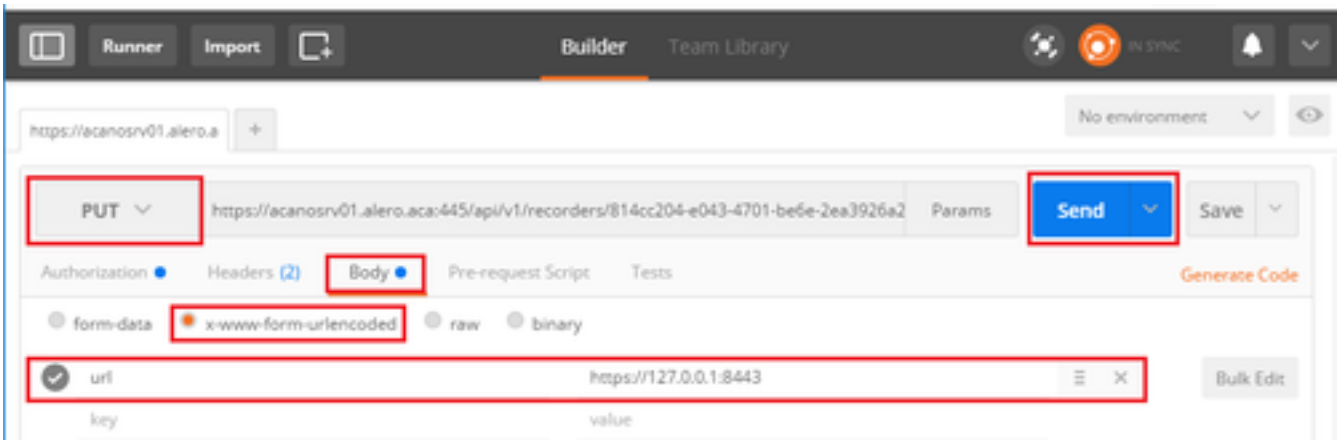
c. Impostare l'URL del registratore inviando un PUT con https://<Callbridge_IP>:445/api/v1/recorders/<recorderid> e aggiungerlo in BODY prima di eseguire il PUT:

url=https://127.0.0.1:8443 (se il registratore si trova sul CB locale)

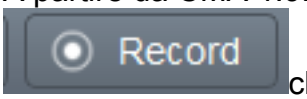
o

url=https://<Indirizzo IP del registratore>:8443 (se il registratore non si trova sul CB locale)

Ad esempio:



Nota: dtmfProfile, **callProfile** e **callLegProfile** sono particolarmente importanti per gli endpoint SIP che partecipano a una conferenza cospace. Consentono all'endpoint di avviare/interrompere la registrazione di una chiamata al/dal cospazio.

A partire da CMA 1.9.3 e CMS 2.0.1, i toni DTMF non sono richiesti ora c'è 

che viene aggiunto al client quando il registratore è presente sul callbridge al quale il client è connesso o ne è a conoscenza. Il pulsante di registrazione è stato aggiunto anche a WebRTC da CMS 2.3.

4. Creare un profilo di chiamata

r. Invia un POST vuoto con **https://<Callbridge_IP>:445/api/v1/callProfiles**

b. Inviare un GET con lo stesso URL in (a), copiare l'ID profilo chiamata, senza virgolette, nel Blocco note

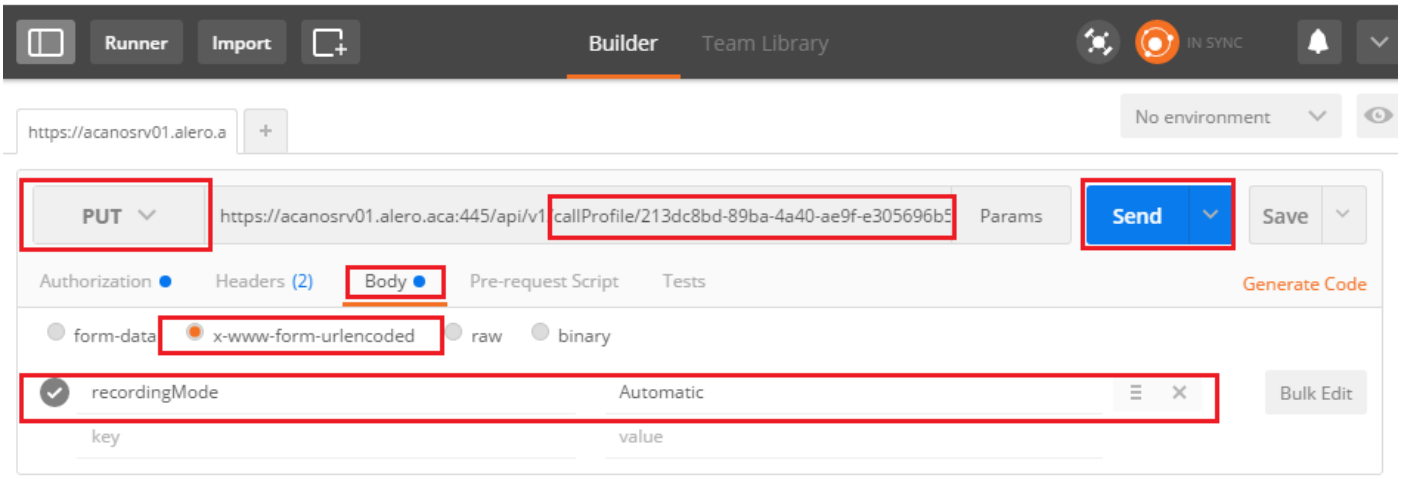
c. Impostare recordingMode su callProfile inviando un PUT con **https://<Callbridge_IP>:445/api/v1/callProfiles/<call profile ID>** e aggiungere il nel BODY prima di eseguire il PUT.

recordingMode=Manuale (se si desidera che i chiamanti avviino la registrazione utilizzando le voci DTMF)

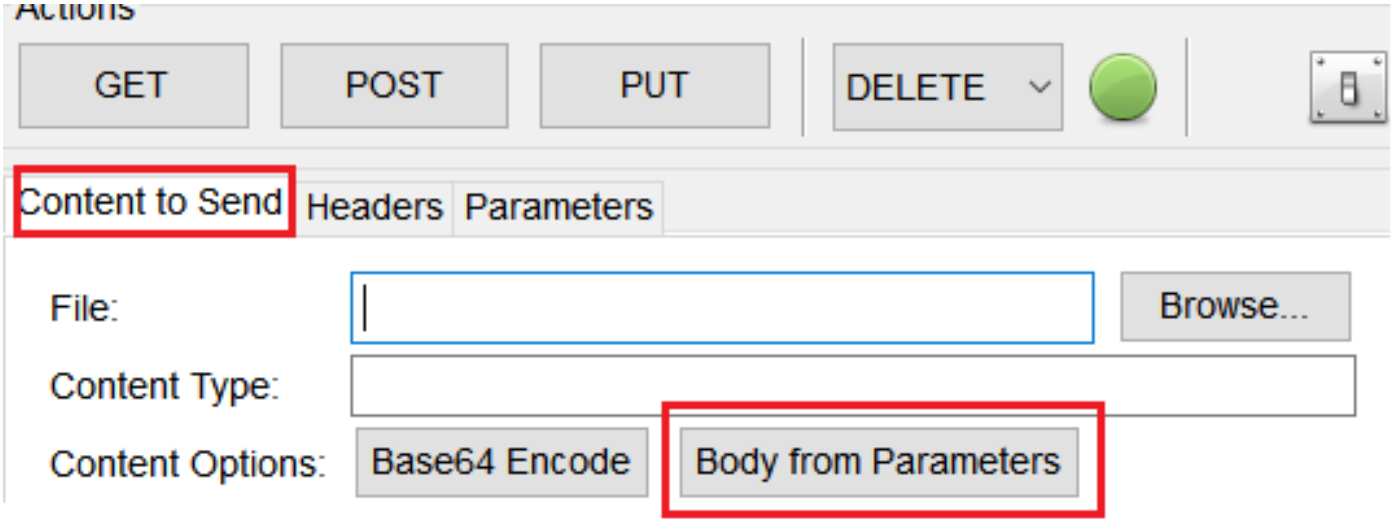
o

recordingMode=Automatic (se la registrazione deve essere avviata automaticamente quando vengono avviate le chiamate)

Ad esempio:



Nota: Se si utilizza POSTER da firefox, è necessario selezionare **Contenuto da inviare** quindi selezionare **Corpo da Parametri** prima di inviare il PUT/POST, in questo modo viene compilato nei codici che la CB può comprendere. Come nell'immagine seguente:



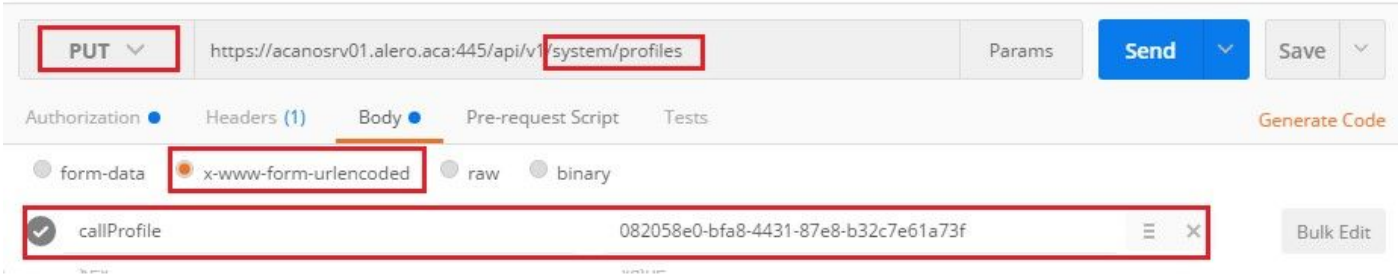
5. Aggiungere il profilo di chiamata ai profili di sistema

Il profilo di chiamata definisce se le chiamate possono essere registrazioni e se possono essere effettuate con o senza l'intervento dell'utente.

Inviare un PUT con https://<Callbridge_IP>:445/api/v1/system/profiles dopo aver aggiunto callProfile in BODY

callProfile=<ID profilo chiamata>

Ad esempio:

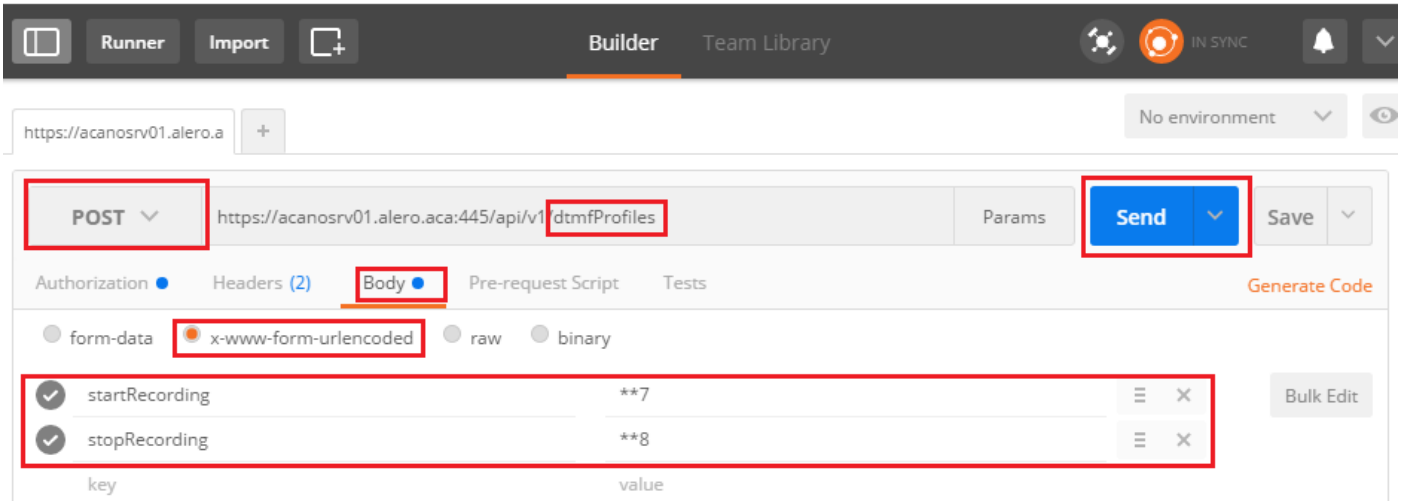


Se la modalità di registrazione è impostata su Manuale, è necessario impostare un profilo DTMF per definire come gli utenti possono avviare e interrompere le registrazioni utilizzando toni DTMF.

6. Creare il profilo DTMF

r. Inviare un post con https://<Callbridge_IP>:445/api/v1/dtmfProfiles dopo aver impostato startRecording=**7 e stopRecording=**8 (ad esempio) in BODY come startRecording=**7&stopRecording=**8.

Ad esempio:



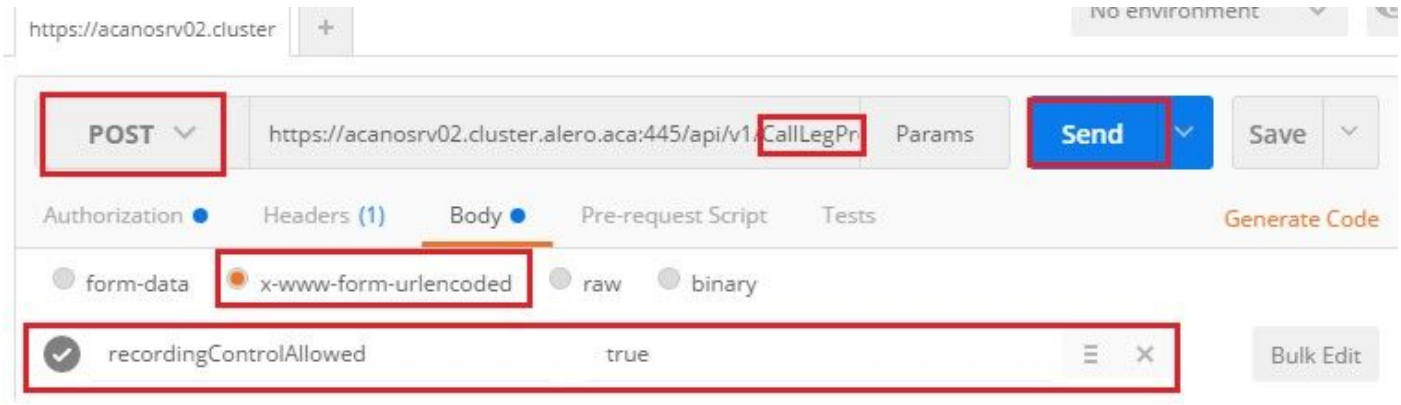
b. Inviare GET per visualizzare il nuovo profilo DTMF, quindi copiare l'ID senza virgolette nel Blocco note.

7. Crea profilo CallLeg

CallLegProfiles determina il comportamento della chiamata. In questo caso determina se è possibile registrare una chiamata.
Creare un profilo della gamba di chiamata come segue:

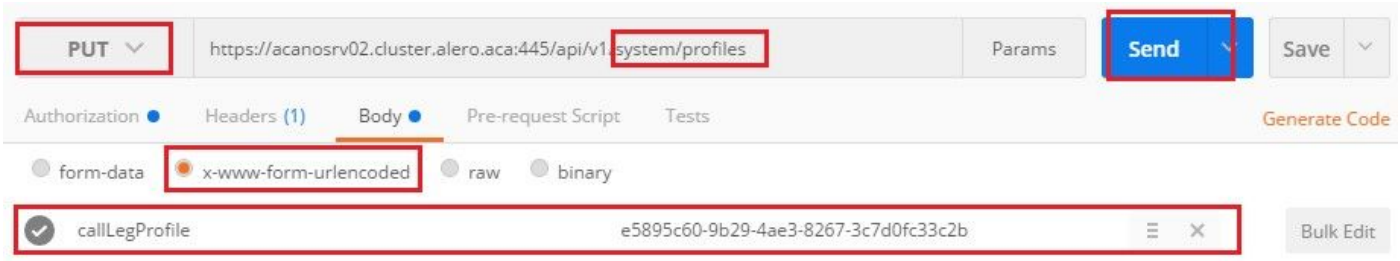
r. Inviare un post con https://<Callbridge_IP>:445/api/v1/CallLegProfiles dopo aver aggiunto recordingControlAllowed=true in BODY:

Ad esempio:



b. Applicare CallLegProfile, inviando un PUT con https://<Callbridge_IP>:445/api/v1/system/profiles e aggiungendo callLegProfile=<callLegProfile_ID> in BODY:

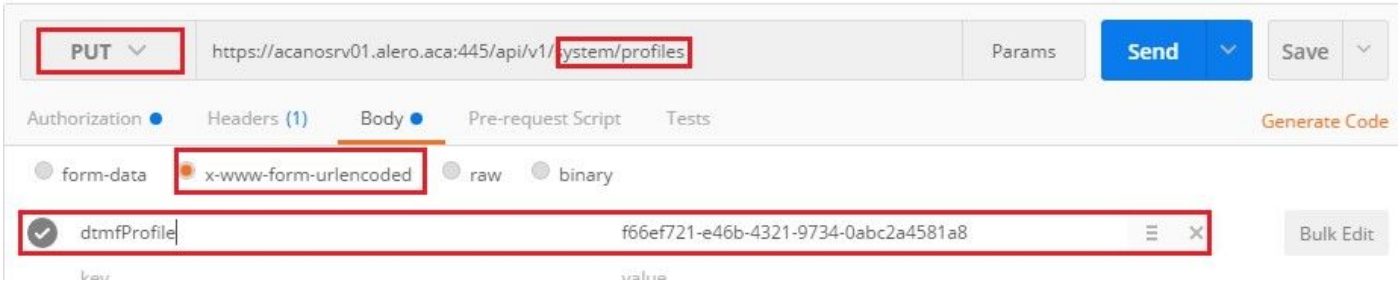
Ad esempio:



8. Applicare il profilo DTMF:

Inviare un PUT con https://<Callbridge_IP>:445/api/v1/system/profiles dopo aver aggiunto dtmfProfile in BODY dtmfProfile=<ID profilo dfmt>

Ad esempio:



Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente

1. Una volta configurato, controllare il suo stato con questi comandi, è possibile ottenere un output simile a quello della prossima immagine

registratore

CB locale autonomo:

```
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
```

Oppure, se cluster, 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. Inviare un GET per visualizzare il profilo di sistema, è necessario visualizzare **callProfile**, **CallLegProfile** e **dtmfProfile** (supponendo che tutti questi siano stati configurati) nel risultato con

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

Ad esempio:

```
1 <?xml version="1.0"?>
2 <profiles>
3     <callLegProfile>9591bd29-dc78-4656-bab1-328b2fd505fe</callLegProfile>
4     <callProfile>cf8cf197-a314-4c2e-93d5-4400551efcd6</callProfile>
5     <dtmfProfile>110ed4b0-fcb2-45e1-9b5c-724f7b037b35</dtmfProfile>
6 </profiles>
```

3. Per controllare ciò che è stato configurato sul profilo di chiamata, usare questo sull'API

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

Questo mostra i metodi di registrazione impostati, Automatico o Manuale, come mostrato:

4. Per verificare la configurazione di CallLegProfile, utilizzare questa API

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

Output di esempio:

5. Per controllare ciò che è stato configurato sul profilo DTMF, usare questo sull'API

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

Ciò indica che i metodi di registrazione sono stati impostati, Automatico o Manuale, come mostrato di seguito:

```
<?xml version="1.0"?>
<dtmfProfile id="110ed4b0-fcb2-45e1-9b5c-724f7b037b35">
    <muteSelfAudio></muteSelfAudio>
    <unmuteSelfAudio></unmuteSelfAudio>
    <toggleMuteSelfAudio></toggleMuteSelfAudio>
    <lockCall></lockCall>
    <unlockCall></unlockCall>
    <muteAllExceptSelfAudio></muteAllExceptSelfAudio>
    <unmuteAllExceptSelfAudio></unmuteAllExceptSelfAudio>
    <endCall></endCall>
    <nextLayout></nextLayout>
    <previousLayout></previousLayout>
    <startRecording>**7</startRecording>
    <stopRecording>**8</stopRecording>
    <allowAllMuteSelf></allowAllMuteSelf>
    <cancelAllowAllMuteSelf></cancelAllowAllMuteSelf>
    <allowAllPresentationContribution></allowAllPresentationContribution>
    <cancelAllowAllPresentationContribution></cancelAllowAllPresentationContribution>
    <muteAllNewAudio></muteAllNewAudio>
    <unmuteAllNewAudio></unmuteAllNewAudio>
    <defaultMuteAllNewAudio></defaultMuteAllNewAudio>
    <muteAllNewAndAllExceptSelfAudio></muteAllNewAndAllExceptSelfAudio>
    <unmuteAllNewAndAllExceptSelfAudio></unmuteAllNewAndAllExceptSelfAudio>
</dtmfProfile>
```

Nota: I profili DTMF non funzionano nelle chiamate punto-punto, quindi è possibile utilizzare solo la registrazione manuale in uno spazio.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per visualizzare gli elementi registrati rispetto al registratore, eseguire il comando:

syslog follow

L'output visualizzato è simile al seguente:

```
Jun 20 20:38:49 kern.info acanosrv05 recorder-proxy[1]:  2016/06/20 20:38:49 Connection from
10.48.54.75:39439: Authentication succeeded
Jun 20 20:38:49 kern.info acanosrv05 recorder-proxy[1]:  2016/06/20 20:38:49 Connection from
10.48.54.75:39439: Connection terminated
Jun 20 20:38:53 kern.info acanosrv05 recorder-proxy[1]:  2016/06/20 20:38:53 Connection from
10.48.54.76:35141: Authentication succeeded
Jun 20 20:38:53 kern.info acanosrv05 recorder-proxy[1]:  2016/06/20 20:38:53 Connection from
10.48.54.76:35141: Connection terminated
```

Nell'esempio, acanosrv05 è il server che ospita il registratore e gli altri nodi CB che si connettono a esso sono 10.48.54.75 e 10.48.54.76.

Ciò dimostra che il CB remoto si sta collegando e autenticando correttamente con il registratore.

Se il registratore è locale rispetto al CB, la connessione viene dall'IP di loopback:

```
Jun 20 20:40:52 kern.info acanosrv01 recorder-proxy[1]:  2016/06/20 20:40:52 Connection from
127.0.0.1:45380: Authentication succeeded
Jun 20 20:40:52 kern.info acanosrv01 recorder-proxy[1]:  2016/06/20 20:40:52 Connection from
127.0.0.1:45380: Connection terminated
```

> **Nota:** La maggior parte dei log relativi ai processi del registratore vengono mostrati nel syslog come proxy del registratore, che fornisce un'indicazione su dove il registratore potrebbe guastarsi.

Altri syslog sono mostrati come segue per il registratore:

In questo caso viene individuato un dispositivo di registrazione e la registrazione viene avviata automaticamente:

```
Jun 20 21:16:19 user.info acanosrv02 host:server:  INFO : recording device 1: available (1
recordings)
```

Se la registrazione non riesce, verificare se è stato trovato un dispositivo di registrazione:

```
Jun 20 21:16:19 user.info acanosrv02 host:server:  INFO : No recording device found
```

Se viene visualizzato un avviso di questo tipo, controllare il certificato nell'attendibilità del registratore per verificare che sia quello corretto utilizzato per configurare il certificato CB.

Controllare il syslog per verificare se lo storage NFS è montato:

- Se lo storage NFS non è montato, viene visualizzato il messaggio "Failed to mount NFS storage" (Impossibile montare lo storage NFS)
- Verificare e assicurarsi che la cartella NFS impostata sul server di registrazione:/Folder-name sia uguale a quella configurata sullo storage NFS

Eseguire l'API per controllare gli allarmi relativi al registratore:

- **https://<callBridge_IP>api/v1/system/alarms**
- Se lo spazio su disco è insufficiente, viene visualizzato "recorderLowDiskSpace"
- Verificare quindi che lo spazio su disco dello storage NFS a cui fa riferimento il registratore sia sufficiente

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems