Recorder configureren in CMS/Acano Call Bridge

Inhoud

Inleiding

In dit document worden de configuratiestappen beschreven die nodig zijn om de Recorder in de Call Bridge (CB)-component van een Cisco Meeting Server (CMS) in te stellen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CMS 1.9 of hoger
- Postman van Google Chrome
- CMS-toepassingsprogrammainterface (API)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

De CMS Recorder is beschikbaar vanaf release 1.9 van de CMS (voorheen Acano) server. De recorder biedt de mogelijkheid om vergaderingen op te nemen en de opnames op een NFS-documentopslag (Network File System) op te slaan.

De recorder gedraagt zich als een Extensible Messaging and Presence Protocol (XMPP) client, dus de XMPP server moet op de server die de Call Bridge ontvangt, zijn ingeschakeld.

Er is een recorder-licentie nodig en deze moet worden toegepast op de CallBridge-component en niet op de Recorder-server.

U hebt een NFS-map (Network File System) nodig en deze kan worden ingesteld op Windows Server of Linux.

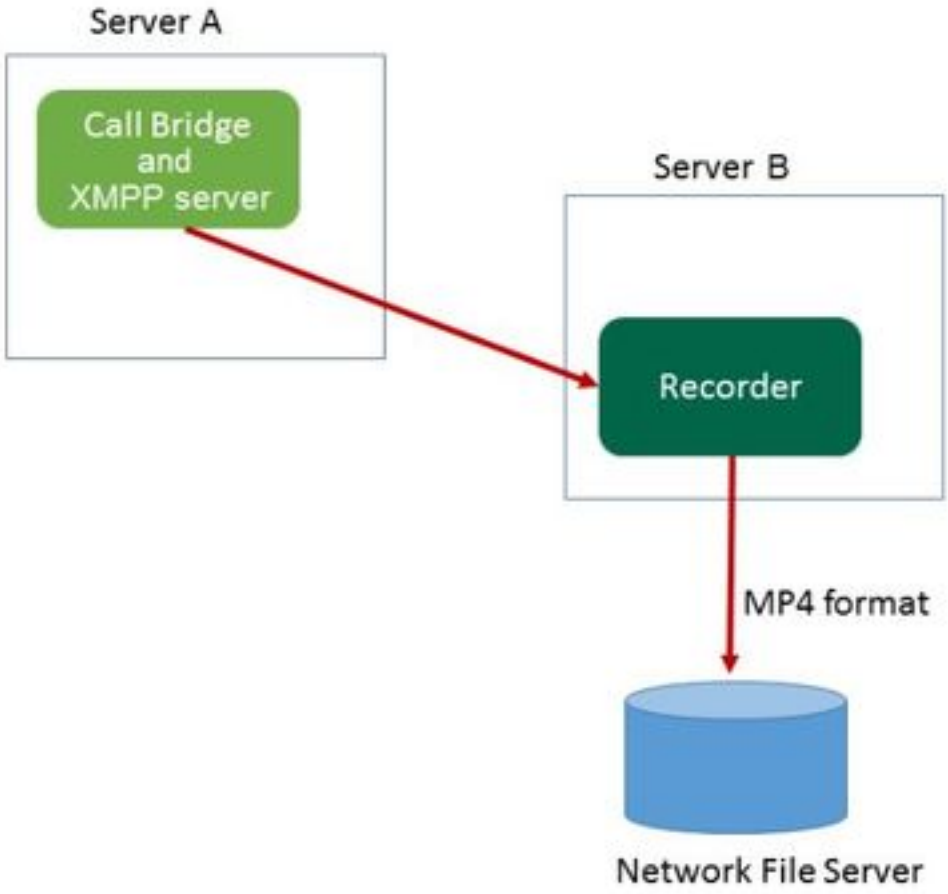
- Voor Windows server volgt u de stappen om netwerkbestandssysteem op Windows te implementeren
- Volg voor Linux de stappen om netwerkbestandssysteem te implementeren op Linux

  Opmerking: Voor NFS die op Windows Server 2008 R2 draait, is er een hotfix voor toegangsprobleem.

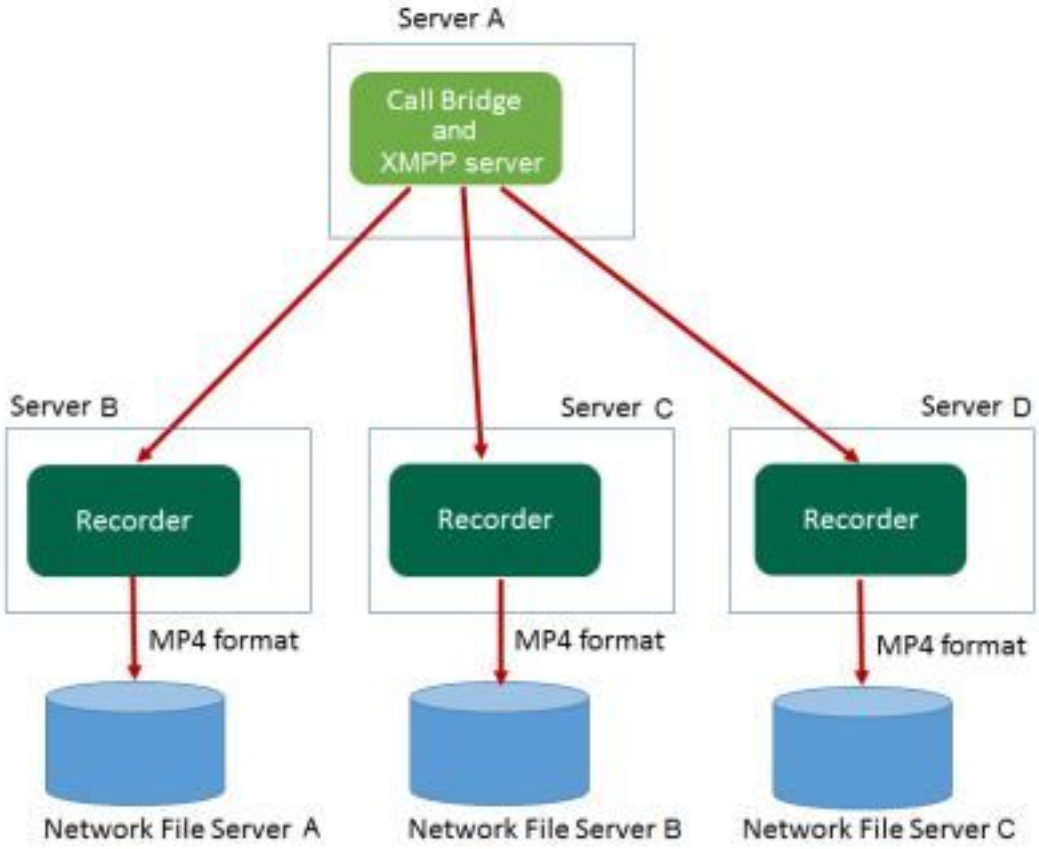
implementaties

Ondersteunde implementaties

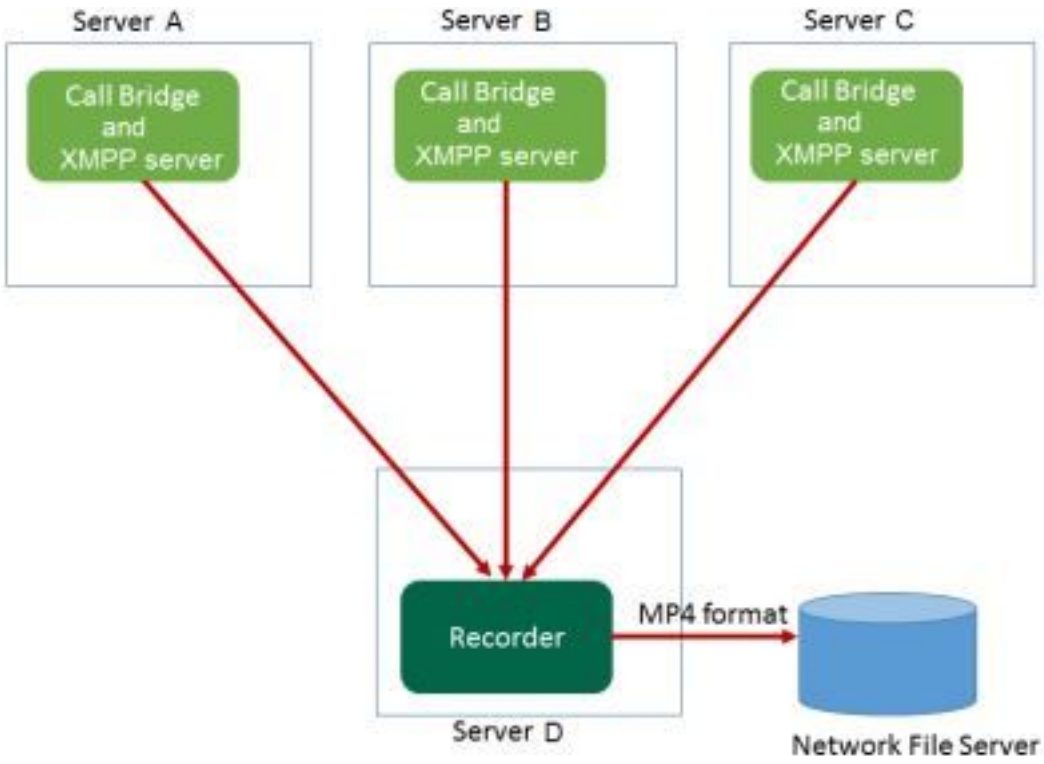
1. De recorder moet worden gehost op een CMS/Acano-server die ver verwijderd is van de server waarop de CB is gevestigd, zoals op deze afbeelding wordt getoond



2. Redundant gebruik van de recorder wordt ook ondersteund. Als redundantie is ingesteld, worden de opnames gebalanceerd tussen alle opnamestation (servers). Dit betekent dat elke CB elke beschikbare recorder gebruikt, zoals in deze afbeelding wordt getoond

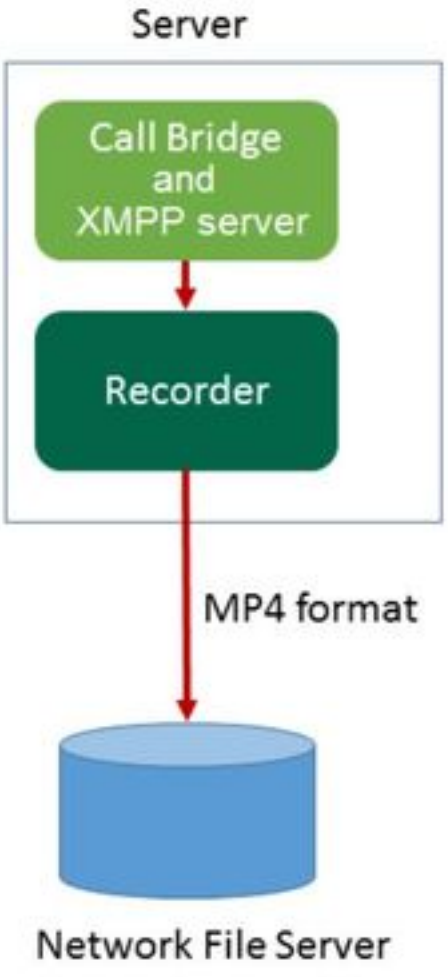


3. Hetzelfde geldt in het tegenovergestelde geval, wanneer er meerdere CB's zijn. Alle CB-knooppunten gebruiken de voor hen beschikbare recorder, zoals in deze afbeelding wordt getoond



Overige instellingen

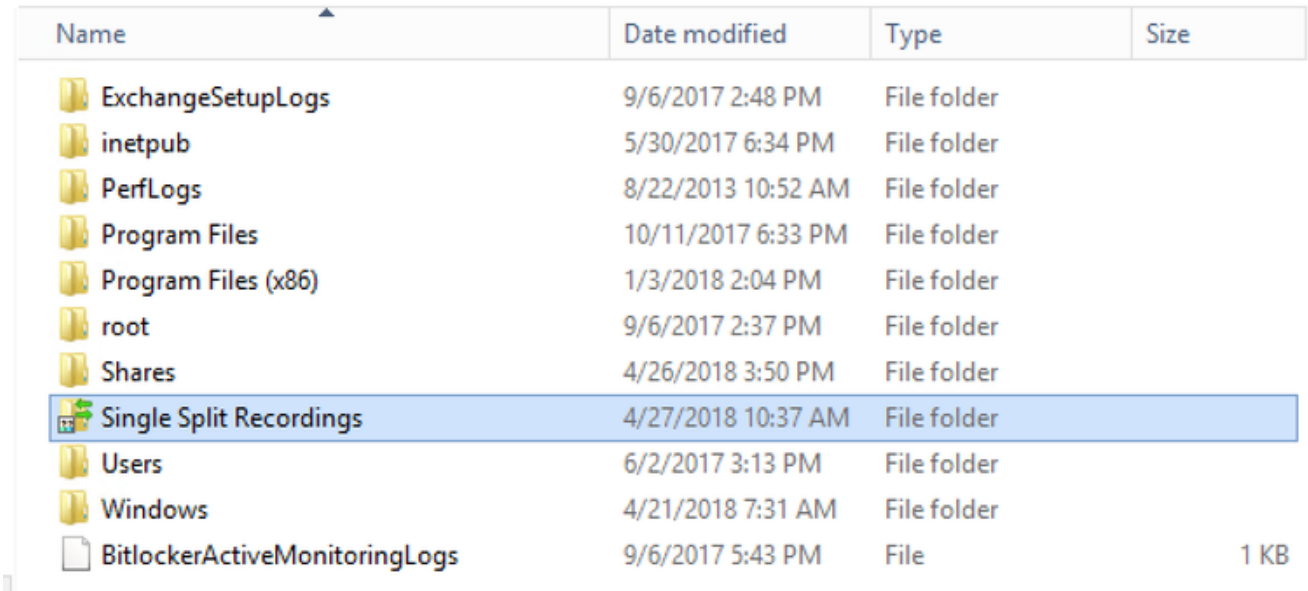
De Recorder kan ook op dezelfde server als de CB worden gehost, maar deze mag alleen worden gebruikt voor tests of zeer kleine implementaties, zie het volgende beeld ter referentie. Hier kan slechts 1-2 simultane opnames worden gemaakt:



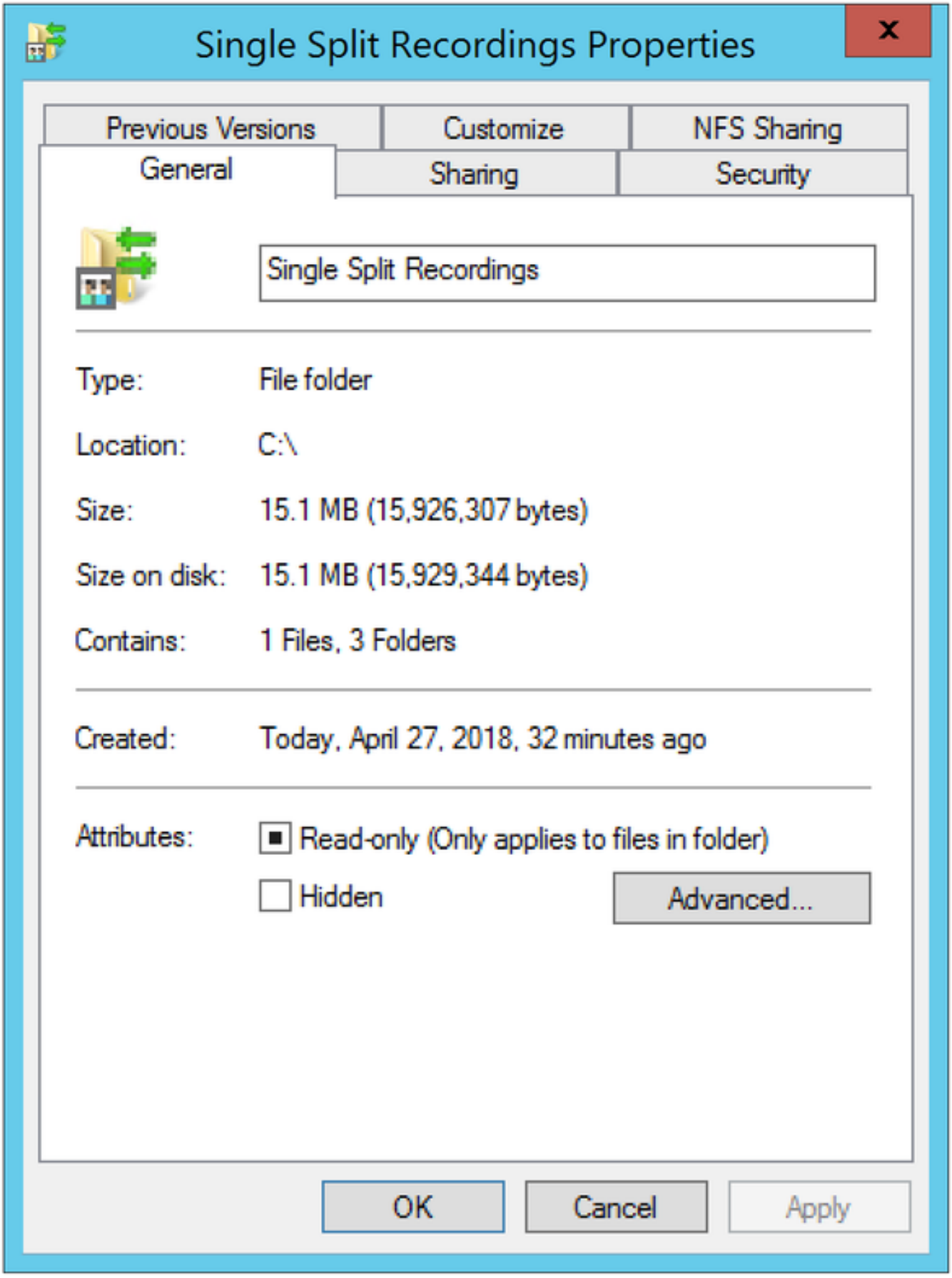
Configureren

Stap 1: Het configureren van een NFS-Share-map op een Windows-server

a. Maak met Windows Verkenner een nieuwe map voor uw NFS-aandeel. In dit voorbeeld is een map met de naam **Enkelvoudige Split-opname** op mijn lokale schijf gemaakt



b. Klik met de rechtermuisknop op de map en selecteer **Eigenschappen**



c. Selecteer het tabblad **NFS**-verdeling rechtsboven. Het toont de map als **Niet gedeeld**. In dit voorbeeld is de map eerder gedeeld, anders moet u een leeg netwerkpad zien en wordt de map weergegeven als **Niet gedeeld**

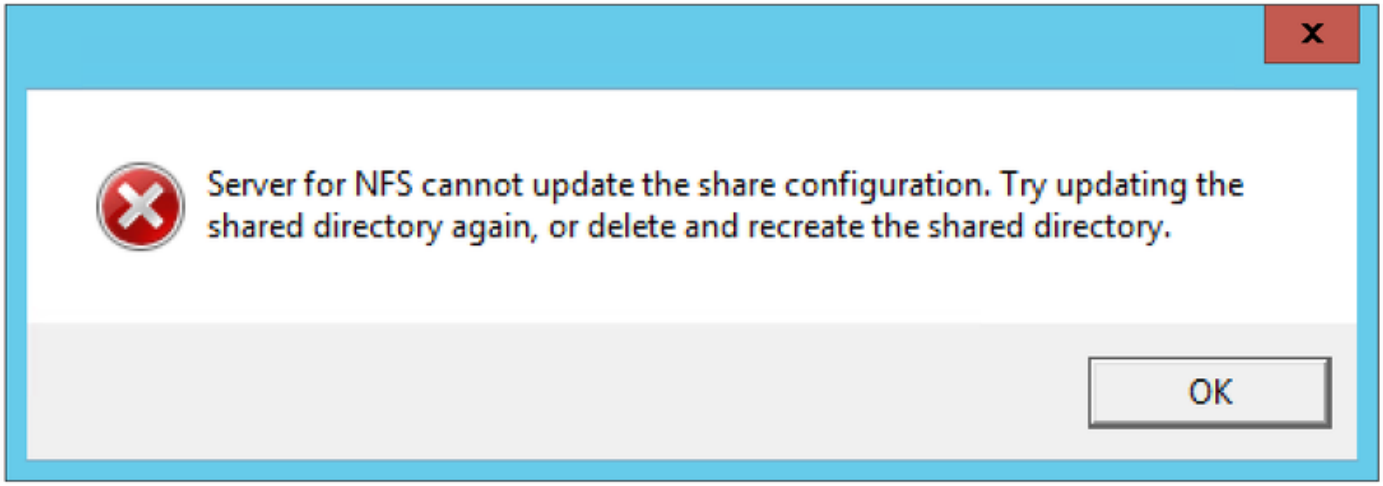
d. Selecteren **NFS-delen beheren**

e. Markeer het selectieteken naast **Deze map delen**

f. Voer de naam van het mappenaandeel in in in **Naam delen** zonder ruimte(n)

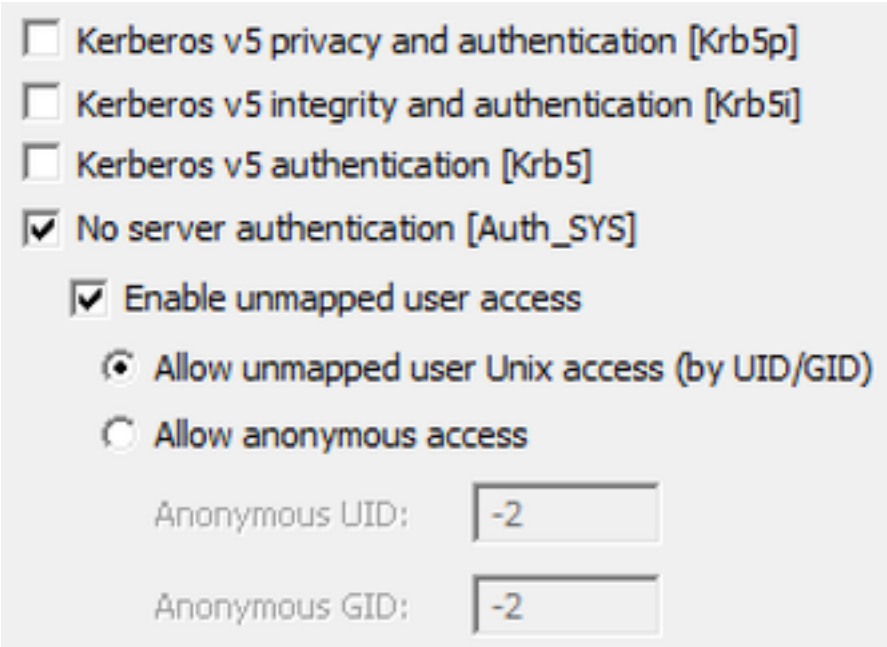
Opmerking: Dit wordt gebruikt door de NFS-cliënten en de CMS-recorder om deze map te vinden.

Opmerking: Zorg ervoor dat er geen ruimte(en) is/zijn in de naam van uw mappenaandeel. Als er een probleem is, kunt u de wijzigingen niet opslaan en verschijnt dit foutenvenster:



g. Laat de codering standaard staan **ANSI** waarderen

h. Standaard worden alle selectietekens gemarkeerd. Schakel alle **Kerberos** Verificatieopties die alleen de **Geen serververificatie [Auth_SYS]**



i. Selecteren **Onin kaart gebrachte gebruiker Unix-toegang toestaan (via UID/GID)**

j. Selecteer onder **Toestemmingen** om rechten in te stellen op het netwerkaandeel

Opmerking: De standaardinstelling is alleen-lezen voor alle machines. De recorder moet toegang tot Lezen-Schrijven hebben, zodat u de standaard voor **ALLE MACHINES** kunt wijzigen of specifieke regels voor uw recorder kunt toevoegen. De beste praktijk zou zijn om toegang tot ALLE MACHINES uit te schakelen door deze in **geen toegang** te veranderen en nieuwe toestemming toe te voegen voor IP van de servers die toegang tot het aandeel nodig hebben.

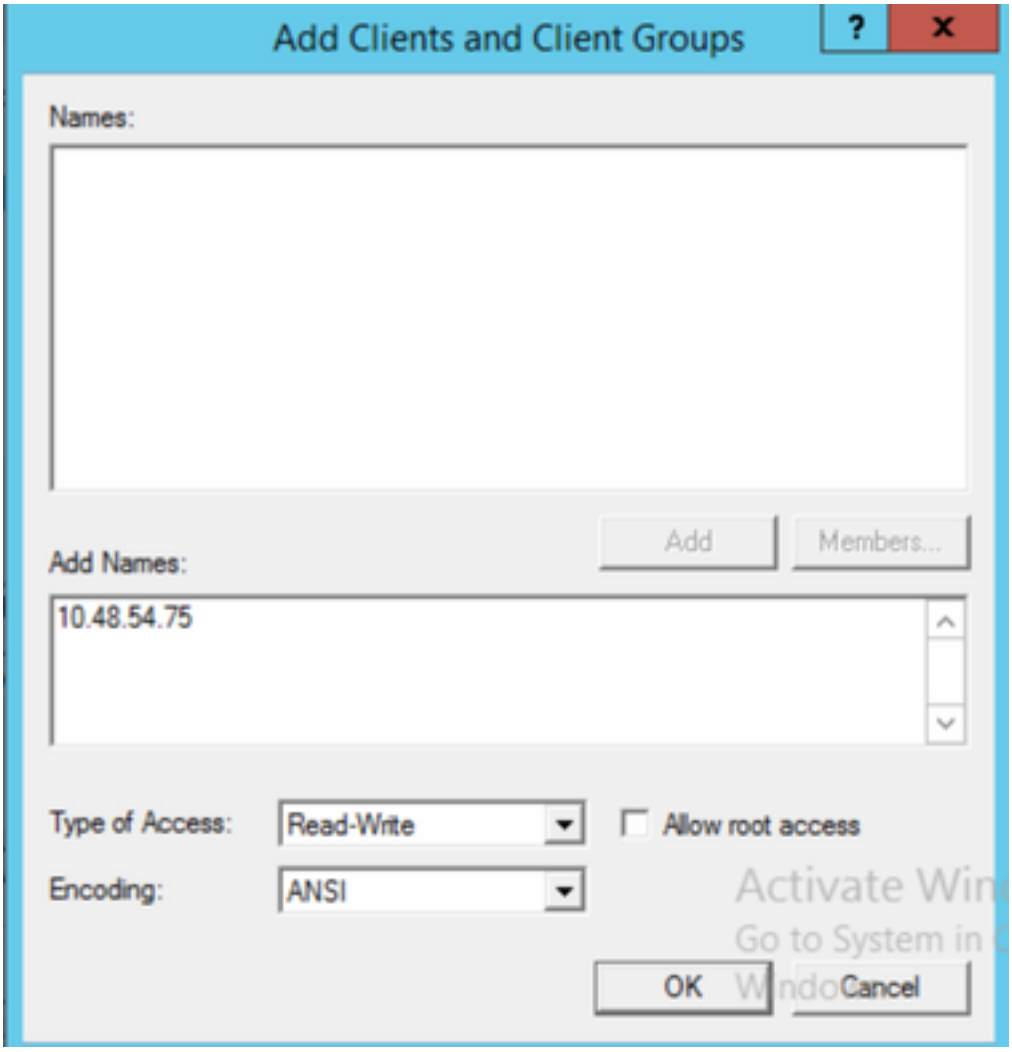
K. Als u toestemming voor uw recorder wilt toevoegen, selecteert u **Toevoegen**

l. In **Namen toevoegen**Voer het IP-adres van uw Recorder server in. In dit voorbeeld is mijn recorder server 10.48.54.75

m. Selecteren **Read-Write** toegang

n. Encodering behouden als **ANSI**

. vertrekken **Toestel worteltoegang** gehandicapt



p. Selecteer **OK** om het dialoogvenster met toegangsrechten te sluiten

V. Selecteren **ALLE MACHINES**

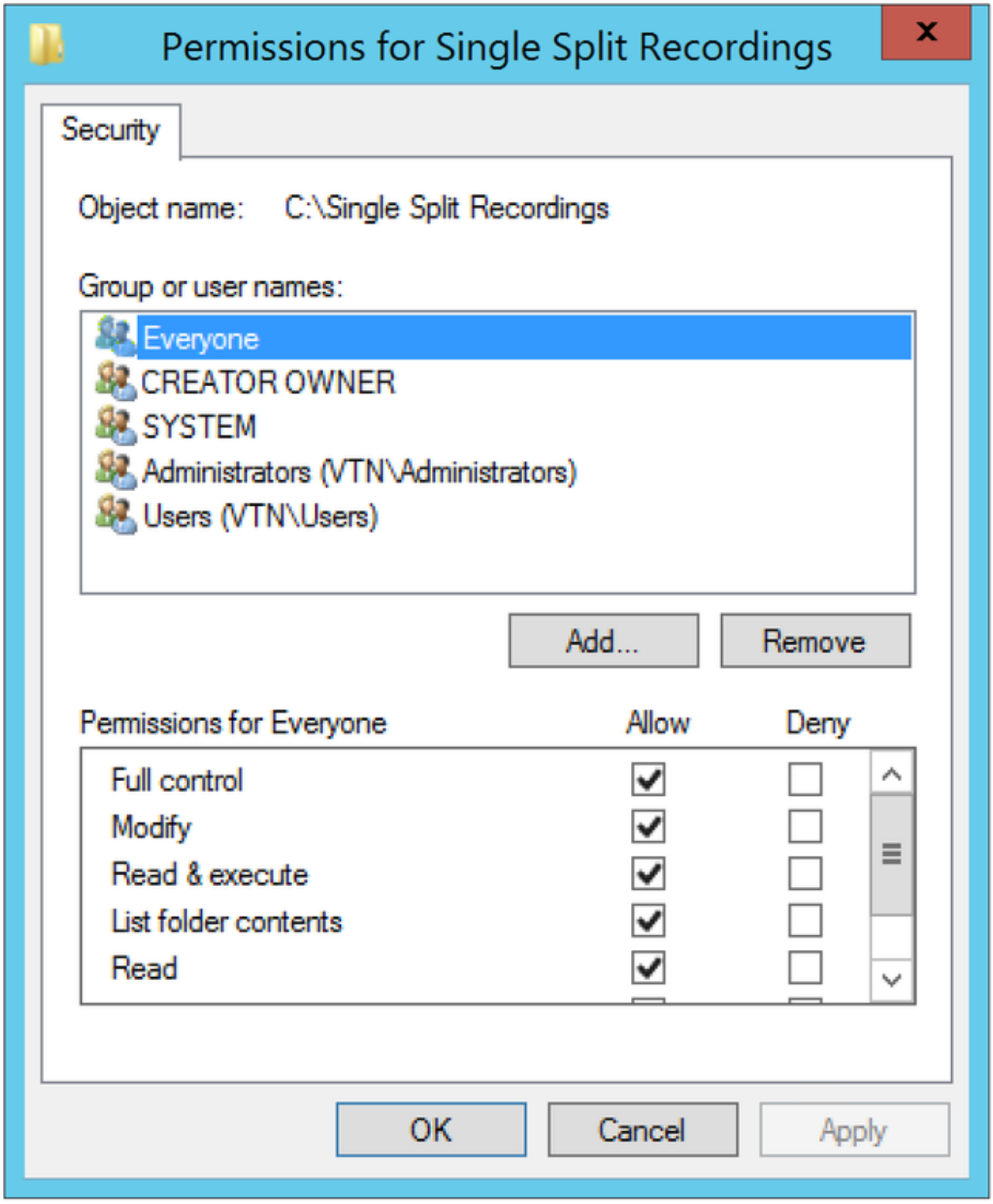
r. Wijzigen **Type toegang** aan **Geen toegang**

s. Selecteren **OK** om het venster voor toegangsrechten te sluiten

t. Selecteren **OK** Opnieuw om naar het venster Mapeigenschappen te keren

u. Selecteren **Security**

Opmerking: De volledige toegang tot de map moet **iedereen** hebben. Als deze niet in de lijst staat, selecteert u **Bewerken** om de editor van toegangsrechten te openen. Selecteer **Toevoegen** om een gebruiker toe te voegen en voer in het veld Naam **Iedereen** de optie OK in. Selecteer **Iedereen** in de lijst en druk op het vakje voor **volledige controle** en selecteer **OK**. Selecteer nogmaals **OK** om de eigenschappen te sluiten. Als het correct is ingesteld, lijkt het op de volgende afbeelding:



Stap 2. Het configureren en inschakelen van de recorder op de recorder server

a. Configuratie van de Recorder om op de interface(s) van uw keuze te luisteren met deze opdracht:

recorder luistert <interface[:port] whitelist>

b. Als de recorder op de lokale CB staat, moet de interface zijn ingesteld op "loopback", dus

gebruik deze opdracht:

recorder luisteren: 8443

c. Als het is om op een specifieke interface te luisteren, laten we dan "a" zeggen, gebruik dan dit:

recorder luisteren a.843

> Opmerking: Als u de recorder op een knooppunt van de geclusterde CB configureren, moet de interface de lokale luisterinterface zijn van het knooppunt waarop de recorder wordt ingesteld.

d. Stel het certificaatbestand in dat door de recorder wordt gebruikt. U kunt een reeds bestaand certificaat en een door de CB gebruikt privé - sleutelbestand gebruiken, bijvoorbeeld.

opnameopdrachten <keybestand> <certificaatbestand>

e. Voeg het CB-certificaat toe aan de Recorder trust store met behulp van de opdracht:

reorder trust <crt-bundle>

De bundel moet het door de CB gebruikte certificaat bevatten, indien verschillend. Indien zich in een cluster bevindt, moet dit de certificaten van elke CB in de cluster bevatten.

f. Specificeer de hostnaam of IP-adres van de NFS en de folder in NFS om de opnames op te slaan:

recorder nfs <hostname/IP>:<folder>

> Opmerking: De Recorder bevestigt niet de NFS-versie, maar het is belangrijk dat de Recorder Server toegang tot de NFS-map heeft gelezen/geschreven.

g. Schakel de recorder in met de opdracht:

recorder

Stap 3. Maak een API-gebruiker op de CB

Maak een API-gebruiker op de CB, dit is vereist voor verdere configuraties met behulp van de API-functie:

Maak de gebruiker met deze stappen:

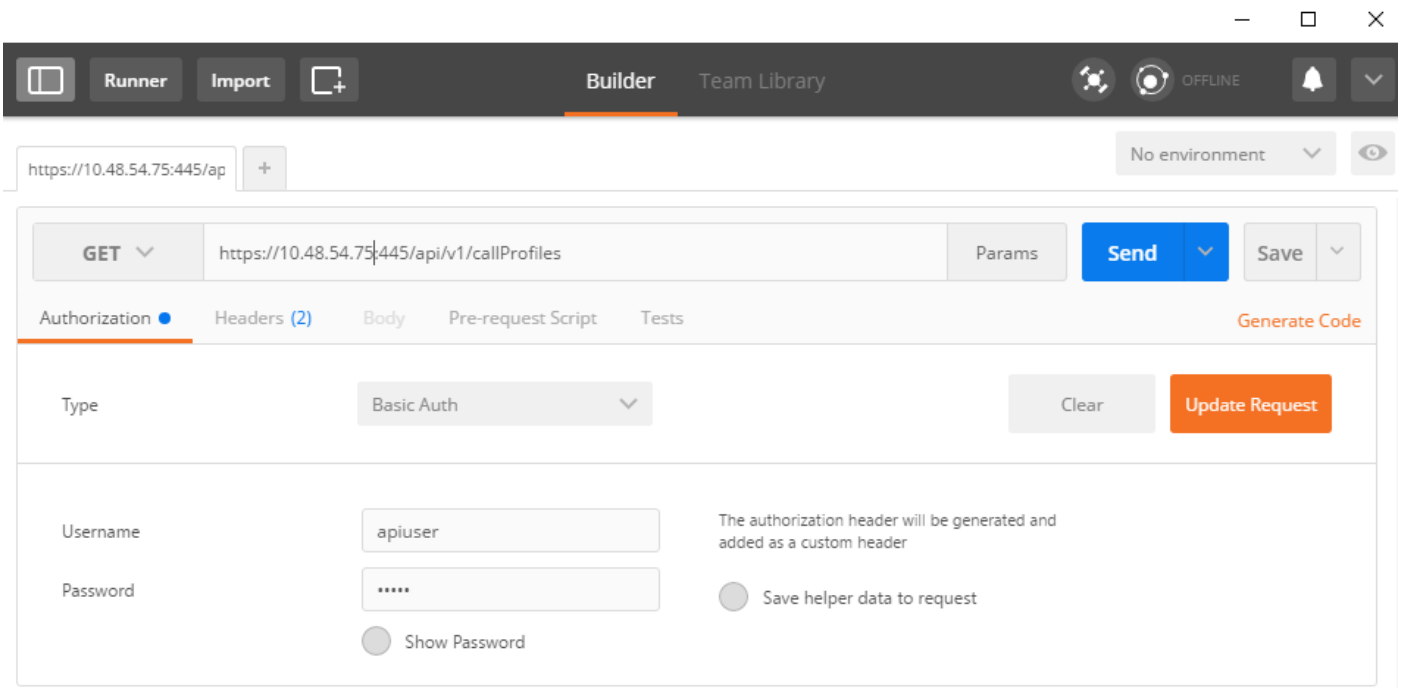
a. Sluit via Secure Shell (SSH) of console aan op de CB met behulp van de admin-referenties.

b. Gebruiker voegt **<gebruikersnaam>** api toe, druk vervolgens op de **Return**-toets en voer het wachtwoord in dat door de **Return**-toets wordt gevolgd.

Stap 4. Voeg de recorder toe aan de CB met behulp van de API

1. Download en installeer Postman van hier

2. Voer de API-toegangsURL in de adresbalk in, bijvoorbeeld: **<Callbridge_IP>:445/API/v1/<entiteit>**. Vervolgens, ingesteld in authenticatie, de gebruikersnaam en het wachtwoord vanaf stap 3, onder autorisatie met **Basic Auth** als type



> Opmerking: Dit veronderstelt dat er momenteel geen recorder of callProfile op de CB is ingesteld. Anders kunt u een recorder wijzigen die bestaat en/of CallProfile aanroepen met behulp van de PUT-methode.

3. Voeg de recorder toe aan de CB met API

a. Verzend een lege POST met https://<Callbridge_IP>:445/API/v1/recorders

b. Stuur een GET met dezelfde URL in (a), kopieer de recorder-ID, zonder de offertes naar Kladblok

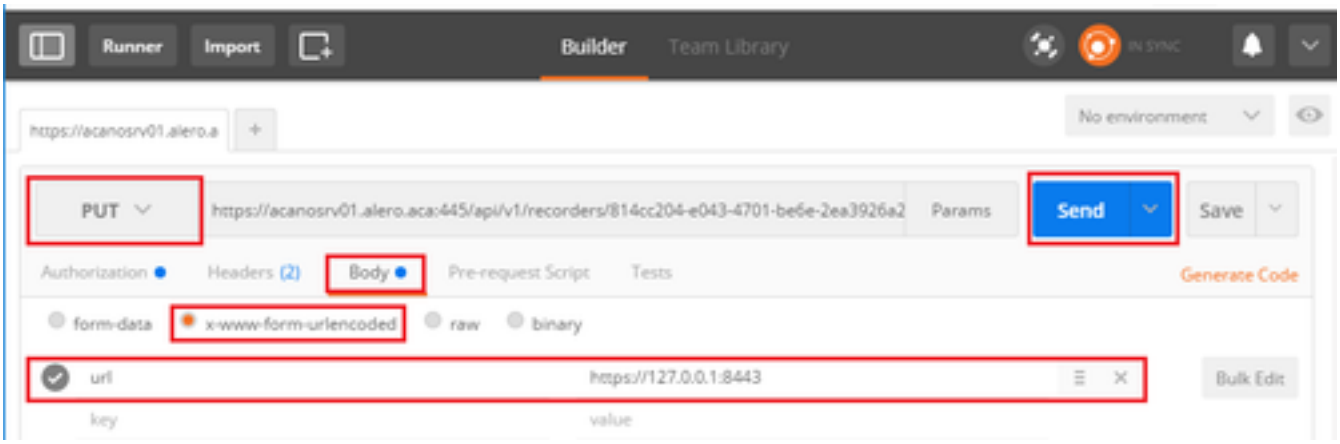
c. Stel de URL van de recorder in door een PUT met https://<Callbridge_IP>:445/api/v1/recorders/<recorderid> te verzenden en voeg dit in BODY toe voordat u de PUT uitvoert:

url=https://127.0.0.1:8443 (indien de recorder op de lokale CB staat)

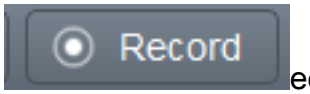
of

URL=https://<IP-adres van recorder>:8443 (indien de recorder niet op de lokale CB is)

Bijvoorbeeld:



Opmerking: **dtmfProfile**, **callProfile** en **callBeenProfile** zijn met name belangrijk voor SIP-endpoints die zich bij een ruimtevaartconferentie aansluiten. Ze staan het Endpoint toe om de opname van een oproep naar/van de ruimte te starten of te stoppen.

Vanaf CMA 1.9.3 en CMS 2.0.1 zijn de DTMF-tonen nu niet vereist 

een toets die aan de client is toegevoegd wanneer de recorder aanwezig is op of bekend is bij de callbridge waarmee de client is verbonden. De opnameknop is ook via CMS 2.3 aan WebexRTC toegevoegd.

4. Een CallProfile maken

a. Verzend een lege POST met **https://<Callbridge_IP>:445/API/v1/CallProfiles**

b. Stuur een GET met dezelfde URL in (a), kopieer de CallProfile ID, zonder de offertes naar Kladblok

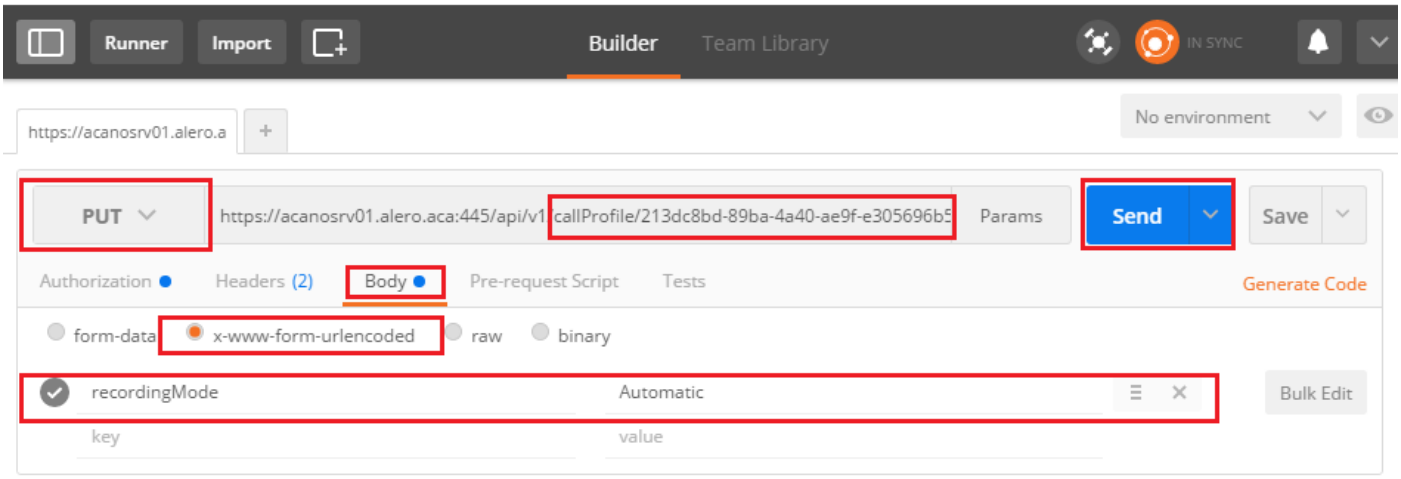
c. Stel de opnameMode in op het CallProfile door een PUT te verzenden met **https://<Callbridge_IP>:445/api/v1/callProfiles/<Call Profile ID>**en voeg de naam in BODY toe voordat u de PUT uitvoert.

opnameMode=Handmatig (als u wilt dat de opbellers beginnen met het opnemen met DTMF-items)

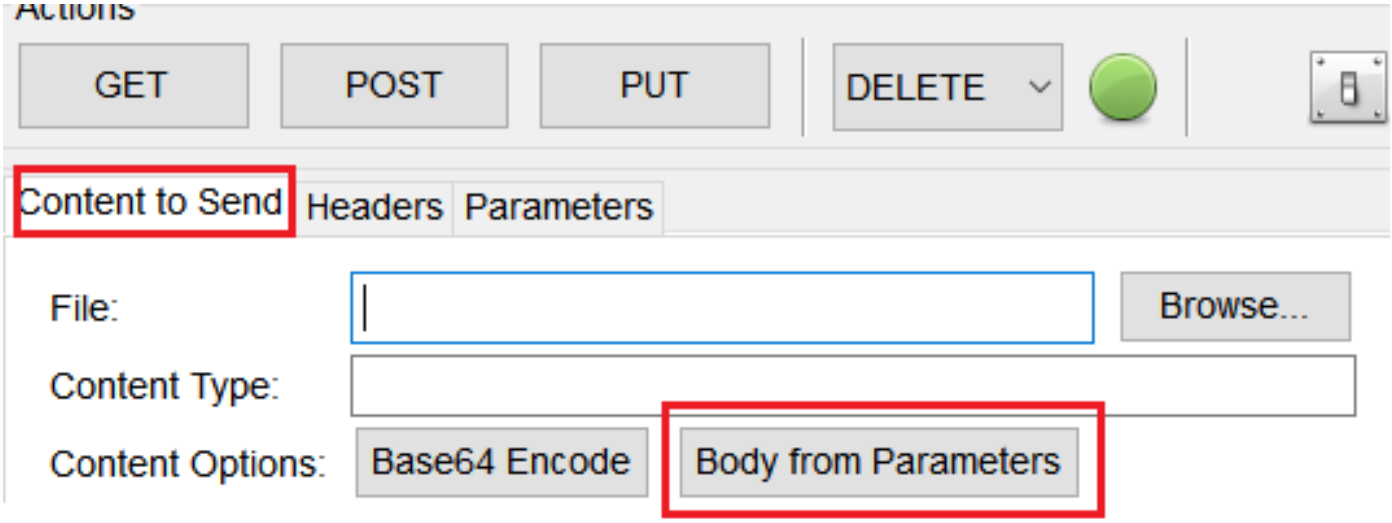
of

opnameMode=Automatisch (indien de opname automatisch moet worden gestart wanneer oproepen worden gestart)

Bijvoorbeeld:



Opmerking: Indien u POSTER uit firefox gebruikt, moet u **Content** selecteren **om** dan **Tekst uit parameters** te selecteren voordat u de PUT/POST verstuurt, zoals deze is gecompileerd in de code(s) die de CB kan begrijpen. Zoals in de volgende afbeelding:



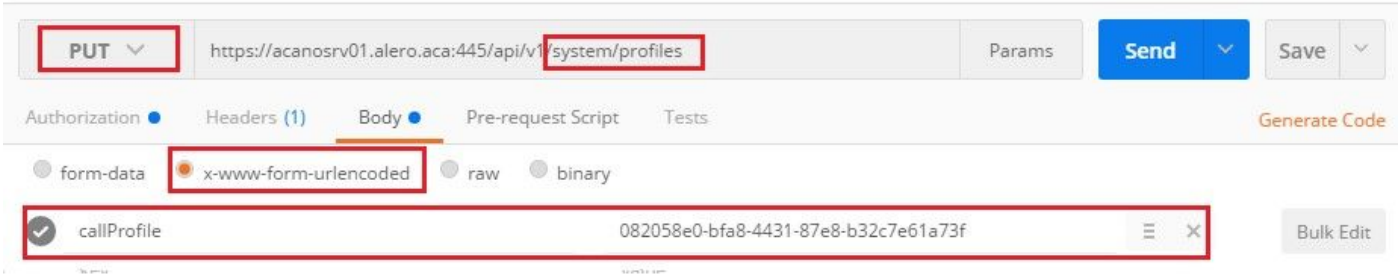
5. Voeg telefoonprofiel toe aan systeemprofielen

CallProfile definieert of de oproepen opnames kunnen zijn en of ze met of zonder gebruikersinterventie kunnen worden gedaan.

Verzend een PUT met https://<Callbridge_IP>:445/API/v1/systeem/profielen nadat u de CallProfile in BODY hebt toegevoegd

CallProfile=<Call Profile ID>

Bijvoorbeeld:

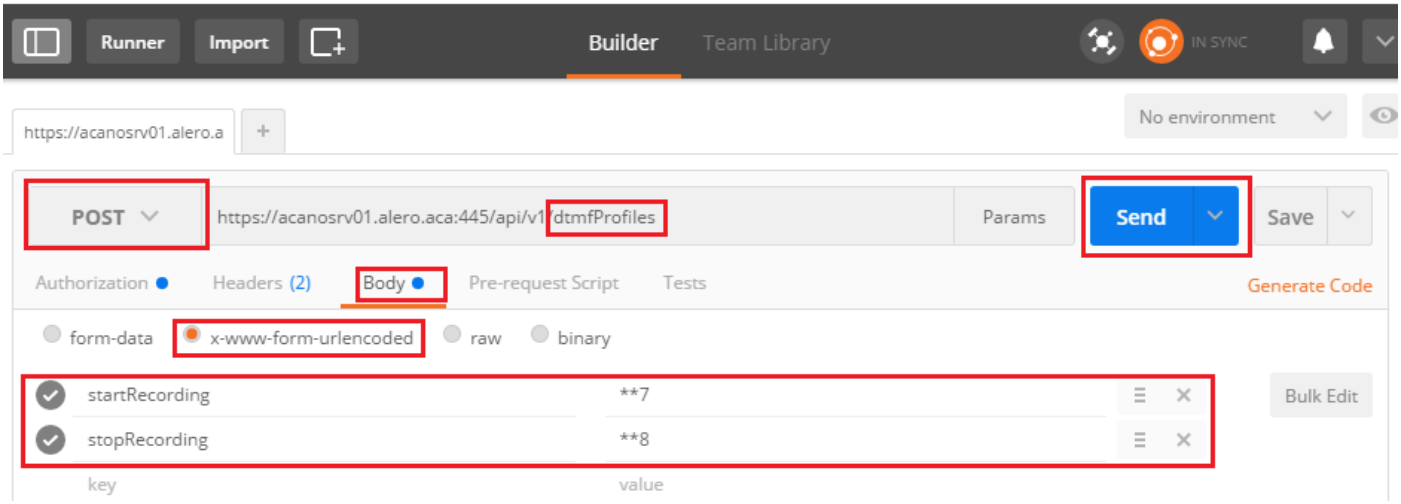


Als de opnameMode op Handmatig is ingesteld, moet u een DTMF-profiel instellen om te definiëren hoe de gebruikers opnames kunnen starten en stoppen met DTMF-tonen.

6. Maak het DTMF-profiel

a. Verzend een post met https://<Callbridge_IP>:445/api/v1/dtmfProfiles nadat u de startRecord=**7 en stopRecord=**8 (bijvoorbeeld) in BODY hebt ingesteld als startRecord=**7&stopRecord=**8.

Bijvoorbeeld:



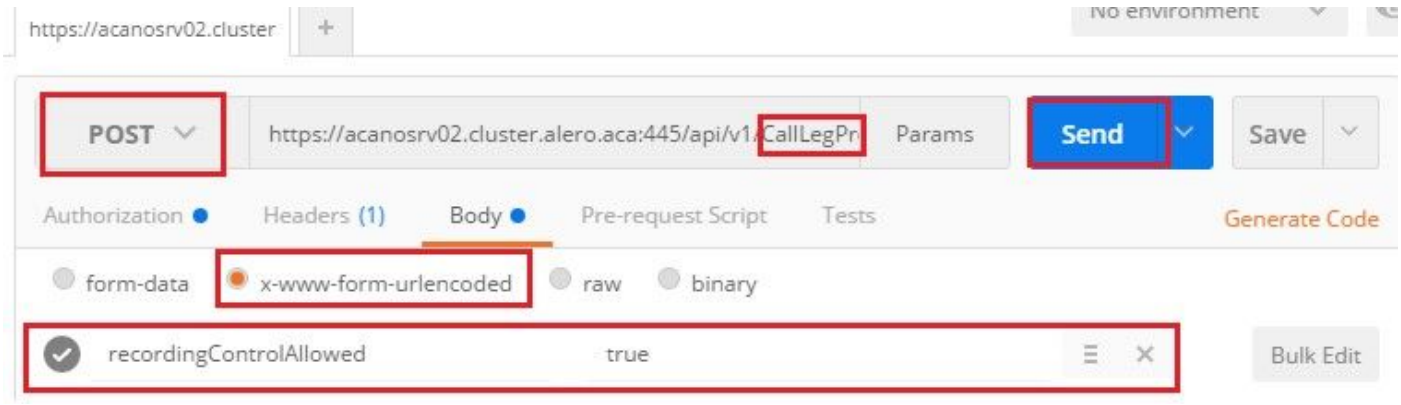
b. Stuur een GET om het nieuwe DTMF-profiel te zien, en kopieer de ID zonder de quotes naar notepad.

7. CallBeen profiel maken

CallBeenProfiles bepaalt het in vraag gedrag. In dit geval bepaalt het of een vraag kan worden geregistreerd.
Maak als volgt een vraagbeenprofiel:

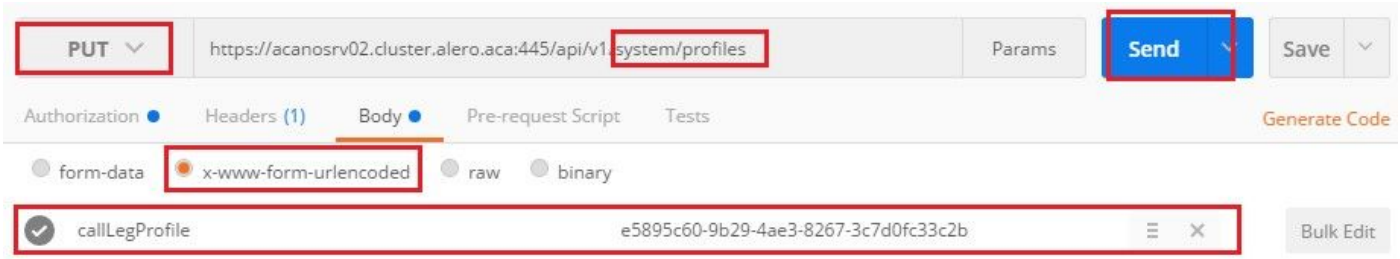
a. Verzend een post met https://<Callbridge_IP>:445/API/v1/CallBeenProfiles nadat u opnameControlAllowed=True in het LICHAAM hebt toegevoegd:

Bijvoorbeeld:



b. Pas het CallBeenProfile toe, door een PUT met https://<Callbridge_IP>:445/API/v1/systeem/profielen te verzenden en CallBeenProfile=<CallBeenProfile_ID> in het LICHAAM toe te voegen:

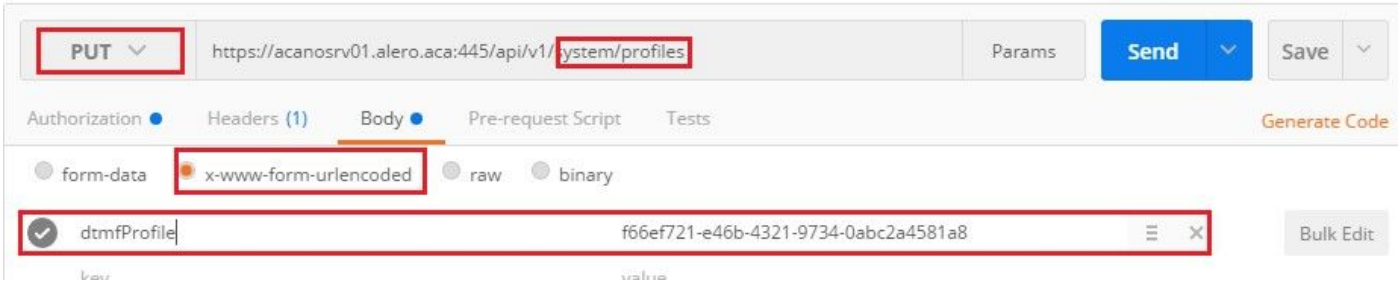
Bijvoorbeeld:



8. Pas het DTMF-profiel toe:

Verzend een PUT met https://<Callbridge_IP>:45/API/v1/systeem/profielen nadat u het dtmfProfile in BODY dtmfProfile=<dfmt Profile ID> hebt toegevoegd

Bijvoorbeeld:



Verifiëren

Gebruik dit gedeelte om te bevestigen dat uw configuratie correct werkt

1. Controleer de status bij deze opdrachten eenmaal, maar u kunt een uitvoer krijgen die vergelijkbaar is met die bij de volgende afbeelding

recorder

Lokale, zelfstandige 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
```

Of indien geclusterde 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. Verzend een GET om het systeemprofiel te bekijken, u moet de **CallProfile**, **CallBeenProfile** en **dtmfProfile** (**ervan uitgaande dat deze allemaal zijn geconfigureerd) in het resultaat** zien met

https://<Callbridge_IP>:445/API/v1/systeem/profielen

Bijvoorbeeld:

```
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. Gebruik deze applicatie op API om te controleren wat er op CallProfile is geconfigureerd

https://<Callbridge_IP>:445/PI/v1/CallProfiles/<CallProfile_ID>

Dit toont de opnamemethoden, hetzij Automatisch of Handmatig, zijn ingesteld, zoals wordt weergegeven:

4. Gebruik deze API om te controleren wat er op CallBeenProfile is geconfigureerd

https://<Callbridge_IP>:445/PI/v1/CallBeenProfiles/<CallBeenProfile_ID>

Uitvoer van voorbeeld:

5. Om te controleren wat op het DTMF-profiel is ingesteld, gebruikt u dit op de API

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

Dit toont aan dat de opnamemethoden (automatisch of handmatig) zijn ingesteld, zoals aangegeven:

```
<?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>
```

> Opmerking: DTMF-profielen werken niet in point to point-call, zodat u alleen handmatige opname in een ruimte kunt gebruiken.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

U kunt de opdracht als volgt weergeven wat er ten opzichte van de recorder wordt geregistreerd:

sysloon

De weergegeven uitvoer is hier gelijk aan:

```
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
```

In dit voorbeeld is acanosrv05 de server die de recorder ontvangt en zijn de andere CB knooppunten die erop aansluiten 10.48.54.75 en 10.48.54.76.

Dit toont aan dat de CB op afstand juist verbindingen maakt en authentiek is met de Recorder.

Als de recorder plaatselijk is aan de CB, dan zou de verbinding van de achterloopback-IP komen:

```
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
```

> Opmerking: De meeste stammen die verband houden met de recorder processen worden in de syslog weergegeven als recorder-volmacht, wat aangeeft waar de recorder mogelijk faalt.

Andere syslogs worden als volgt weergegeven voor de recorder:

In dit geval wordt een opnamestation gevonden en begint de opname automatisch:

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

Als de opname defect is, controleer dan of een opnamestation is gevonden:

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

Indien u een dergelijke waarschuwing ziet, controleer dan het certificaat in de trust van de recorder om er zeker van te zijn dat het de juiste is, gebruikt om de CB te configureren.

Controleer of de syslog is gemonteerd:

- Als de NFS-opslag niet is gemonteerd, wordt "Kan NFS-opslag niet worden geïnstalleerd" weergegeven
- Controleer en zorg ervoor dat de NFS-map op de recorder server is ingesteld:/Folder-name hetzelfde is als wat er is ingesteld in de NFS-opslag

Start API om alarmen te controleren die betrekking hebben op de recorder:

- **https://<CallBridge_IP>API/v1/systeem/alarm**
- Bij een lage schijfruimte wordt "recorderLowDiskSpace" weergegeven
- Controleer vervolgens of de NFS-opslag waarnaar door de recorder wordt verwezen, voldoende schijfruimte heeft

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems