Configurer l'enregistreur dans le pont d'appel CMS/Acano

Contenu

Introduction

Ce document décrit les étapes de configuration nécessaires pour configurer l'enregistreur sur le composant Call Bridge (CB) d'un serveur de réunion Cisco (CMS).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CMS 1.9 ou supérieur
- Postman de Google Chrome
- interface de programmation d’application (API) de CMS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

L'enregistreur CMS est disponible à partir de la version 1.9 du serveur CMS (anciennement Acano). L'enregistreur permet d'enregistrer des téléconférences et d'enregistrer les enregistrements sur un stockage de documents NFS (Network File System).

L'enregistreur se comporte comme un client XMPP (Extensible Messaging and Presence Protocol), de sorte que le serveur XMPP doit être activé sur le serveur qui héberge le pont d'appel.

La licence de l'enregistreur est nécessaire et doit être appliquée sur le composant CallBridge, et non sur le serveur de l'enregistreur.

Le répertoire NFS (Network File System) est nécessaire et peut être configuré sur Windows Server ou Linux.

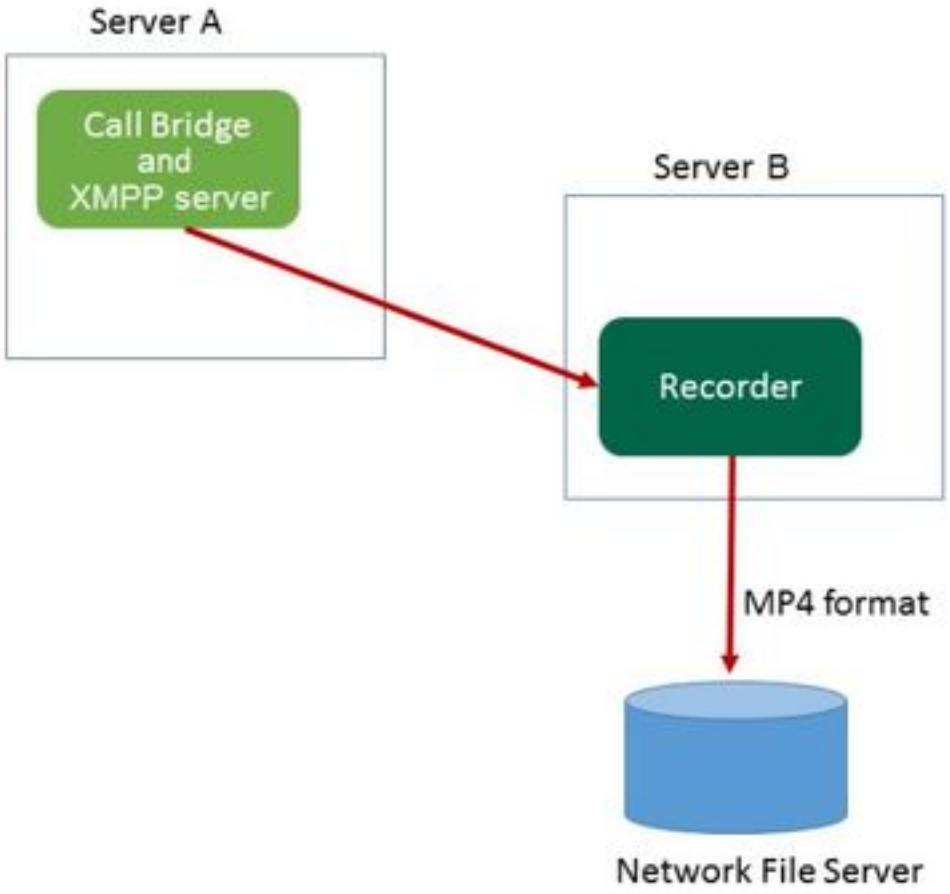
- Pour le serveur Windows, procédez comme suit pour déployer le système de fichiers réseau sous Windows
- Pour Linux, suivez les étapes pour déployer le système de fichiers réseau sous Linux

  Note: Pour NFS qui s'exécute sur Windows Server 2008 R2, il existe un correctif pour le problème d'autorisation.

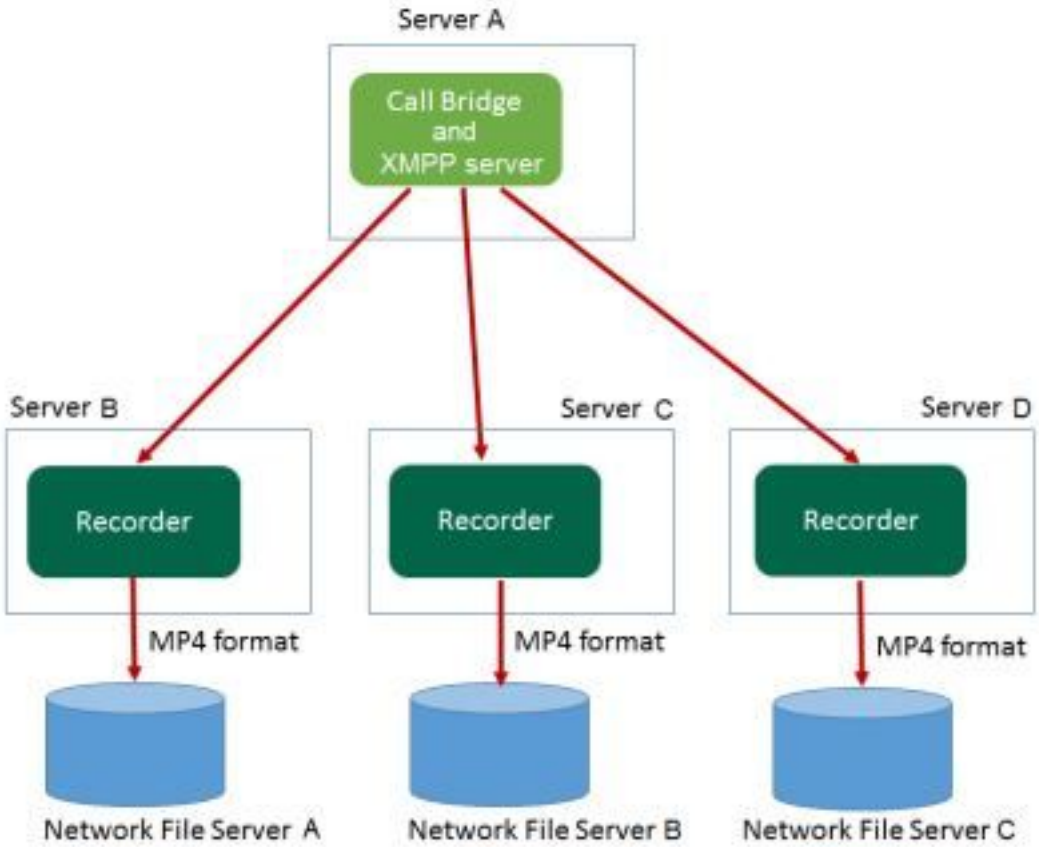
Déploiements

Déploiements pris en charge

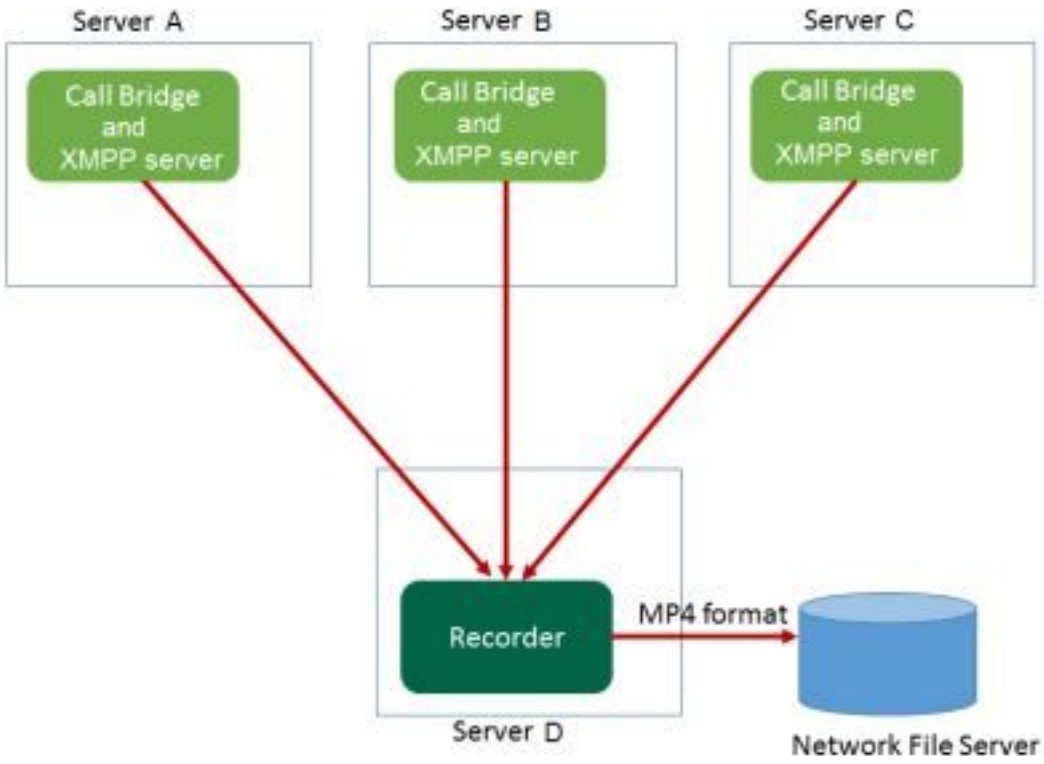
1. L'enregistreur doit être hébergé sur un serveur CMS/Acano distant au serveur qui héberge la CB, comme indiqué sur cette image



2. Le déploiement redondant de l'enregistreur est également pris en charge. Si la redondance est configurée, la charge des enregistrements est équilibrée entre tous les périphériques d'enregistrement (serveurs). Cela signifie que chaque CB utilise chaque Enregistreur disponible, comme illustré sur cette image.

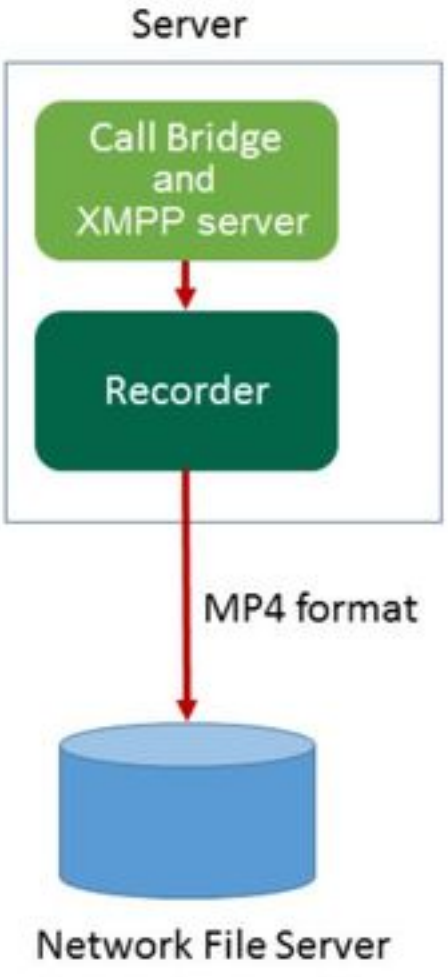


3. Il en va de même au contraire, lorsqu'il y a plusieurs BC. Tous les noeuds CB utilisent l'enregistreur disponible, comme illustré sur cette image



Autre configuration

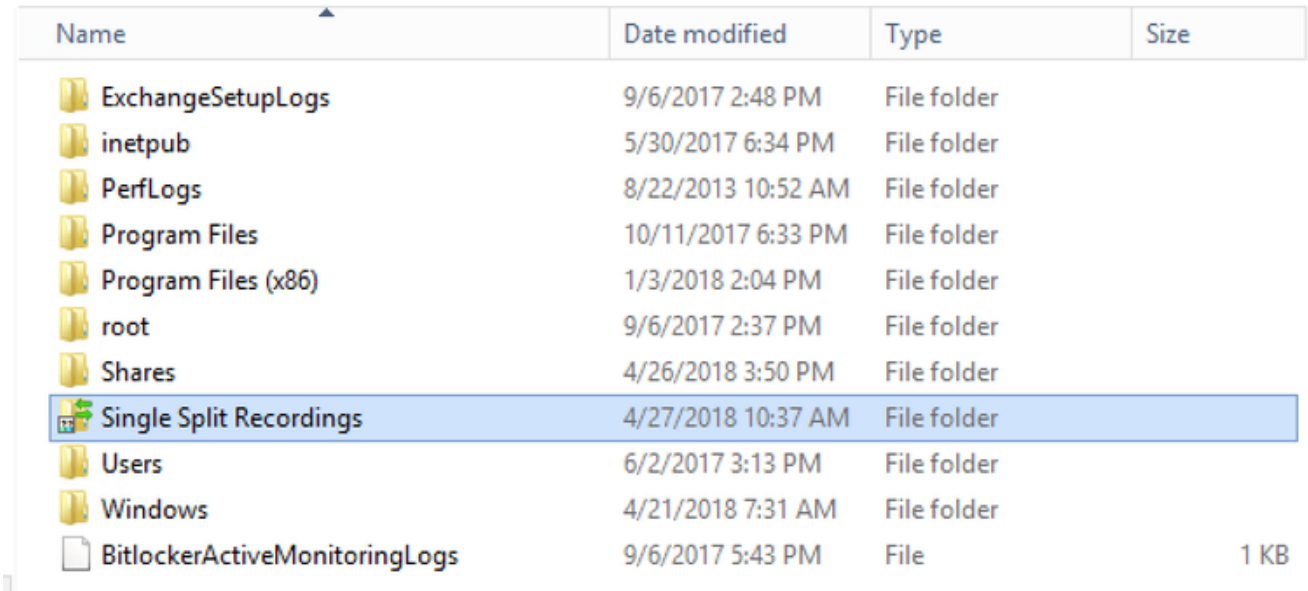
L'enregistreur peut également être hébergé sur le même serveur que la CB, mais il ne doit être utilisé que pour les tests ou les déploiements de très petite taille, voir l'image suivante pour référence. L'inconvénient est que seuls 1 à 2 enregistrements simultanés sont possibles :



Configuration

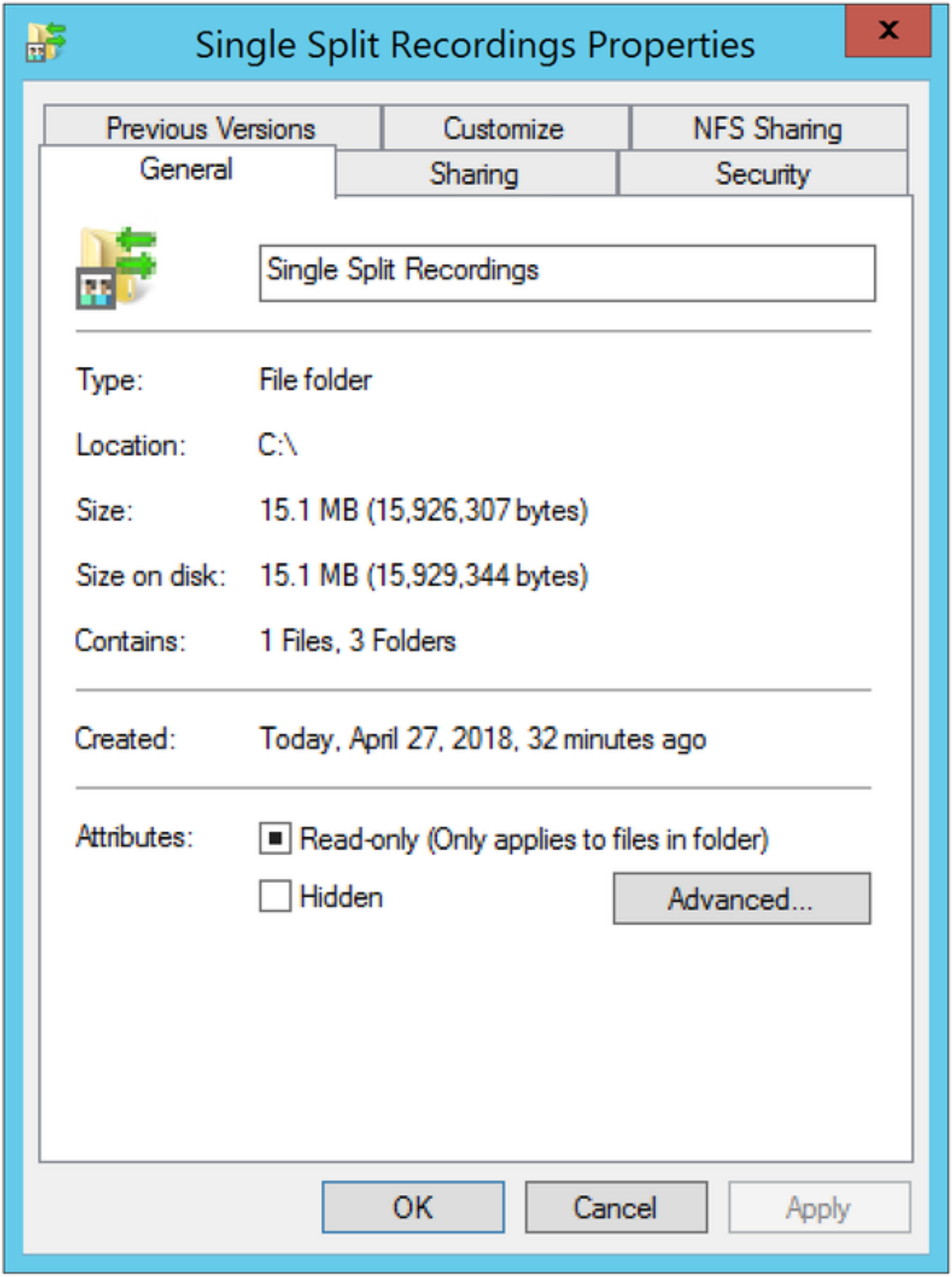
Étape 1. Configurer un dossier de partage NFS sur un serveur Windows

a. À l'aide de l'Explorateur Windows, créez un nouveau dossier pour votre partage NFS. Dans cet exemple, un dossier nommé **Enregistrements fractionnés uniques** a été créé sur mon disque local



Name	Date modified	Type	Size
ExchangeSetupLogs	9/6/2017 2:48 PM	File folder	
inetpub	5/30/2017 6:34 PM	File folder	
PerfLogs	8/22/2013 10:52 AM	File folder	
Program Files	10/11/2017 6:33 PM	File folder	
Program Files (x86)	1/3/2018 2:04 PM	File folder	
root	9/6/2017 2:37 PM	File folder	
Shares	4/26/2018 3:50 PM	File folder	
Single Split Recordings	4/27/2018 10:37 AM	File folder	
Users	6/2/2017 3:13 PM	File folder	
Windows	4/21/2018 7:31 AM	File folder	
BitlockerActiveMonitoringLogs	9/6/2017 5:43 PM	File	1 KB

b. Cliquez avec le bouton droit sur le dossier, puis sélectionnez **Propriétés**



c. Sélectionnez l'onglet **Partage NFS** en haut à droite. Il affiche le dossier comme **Non partagé**. Dans cet exemple, le dossier a déjà été partagé, sinon vous devez voir un chemin d'accès réseau vide et le dossier s'affiche comme **Non partagé**

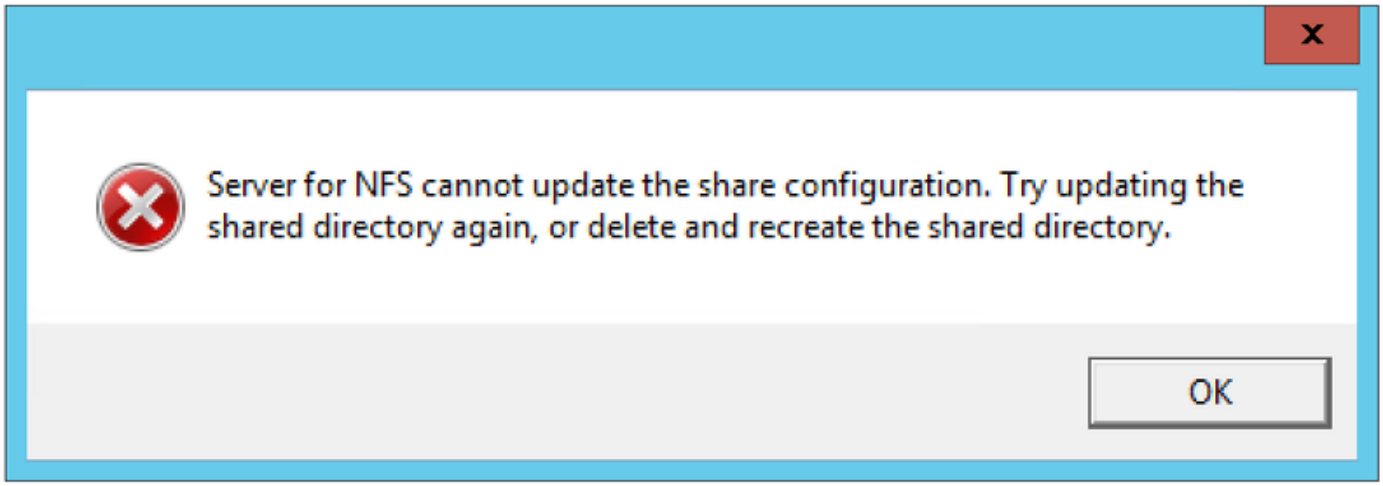
d. Sélectionner **Gérer le partage NFS**

e. Cochez la case en regard de **Partager ce dossier**

f. Entrez votre nom de partage de dossier dans **le nom de partage** sans espace(s)

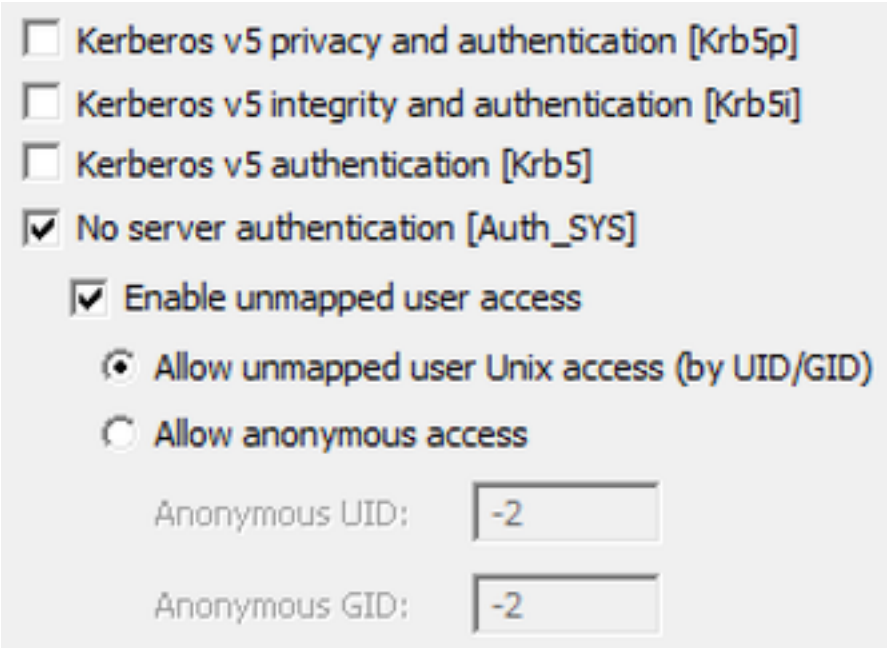
> **Note**: Il est utilisé par les clients NFS et l'enregistreur CMS pour trouver ce dossier.

> **Note**: Assurez-vous qu'il n'y a pas d'espace(s) dans votre nom de partage de dossier. S'il y en a, vous ne pourrez pas enregistrer vos modifications et cette fenêtre d'erreur s'affiche :



g. Laissez le codage à sa valeur par défaut **ANSI** valeur

h. Par défaut, toutes les cases à cocher d'authentification sont marquées. Décochez toutes les **Kerberos** options d'authentification ne laissant que **Aucune authentification de serveur [Auth_SYS]**



i. Sélectionner **Autoriser l'accès Unix utilisateur non mappé (par UID/GID)**

j. En bas, sélectionnez **Autorisations** Pour définir les autorisations sur le partage réseau

> **Note**: La valeur par défaut est Lecture seule pour toutes les machines. L'enregistreur doit

disposer d'un accès en lecture-écriture, de sorte que vous pouvez modifier la valeur par défaut de **TOUTES LES MACHINES**, ou ajouter des règles spécifiques à votre enregistreur. La meilleure pratique serait de désactiver l'accès à TOUTES LES MACHINES en le changeant en **No Access** et en ajoutant de nouvelles autorisations pour l'IP des serveurs qui ont besoin d'accéder au partage.

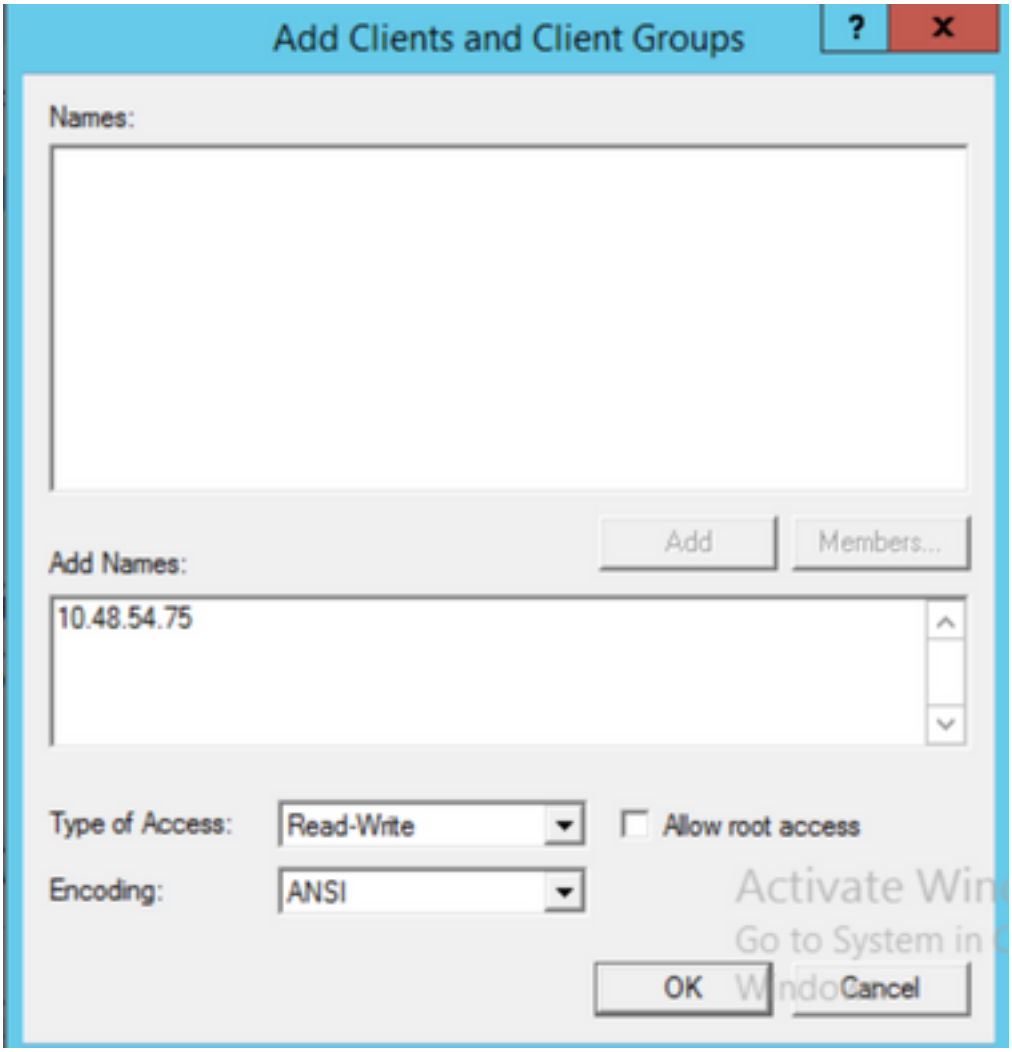
k. Pour ajouter l'autorisation de votre enregistreur, sélectionnez **Ajouter**

l. Dans **Ajouter des noms**, saisissez l'adresse IP de votre serveur Recorder. Dans cet exemple, mon serveur d'enregistreurs est 10.48.54.75

m. Sélectionner **Lecture-Écriture** accès

n. Conserver le codage comme **ANSI**

o. Congé **Autoriser l'accès racine** désactivé



p. Sélectionnez **OK** pour fermer la boîte de dialogue Autorisations.

q. Sélectionner **TOUS LES MACHINES**

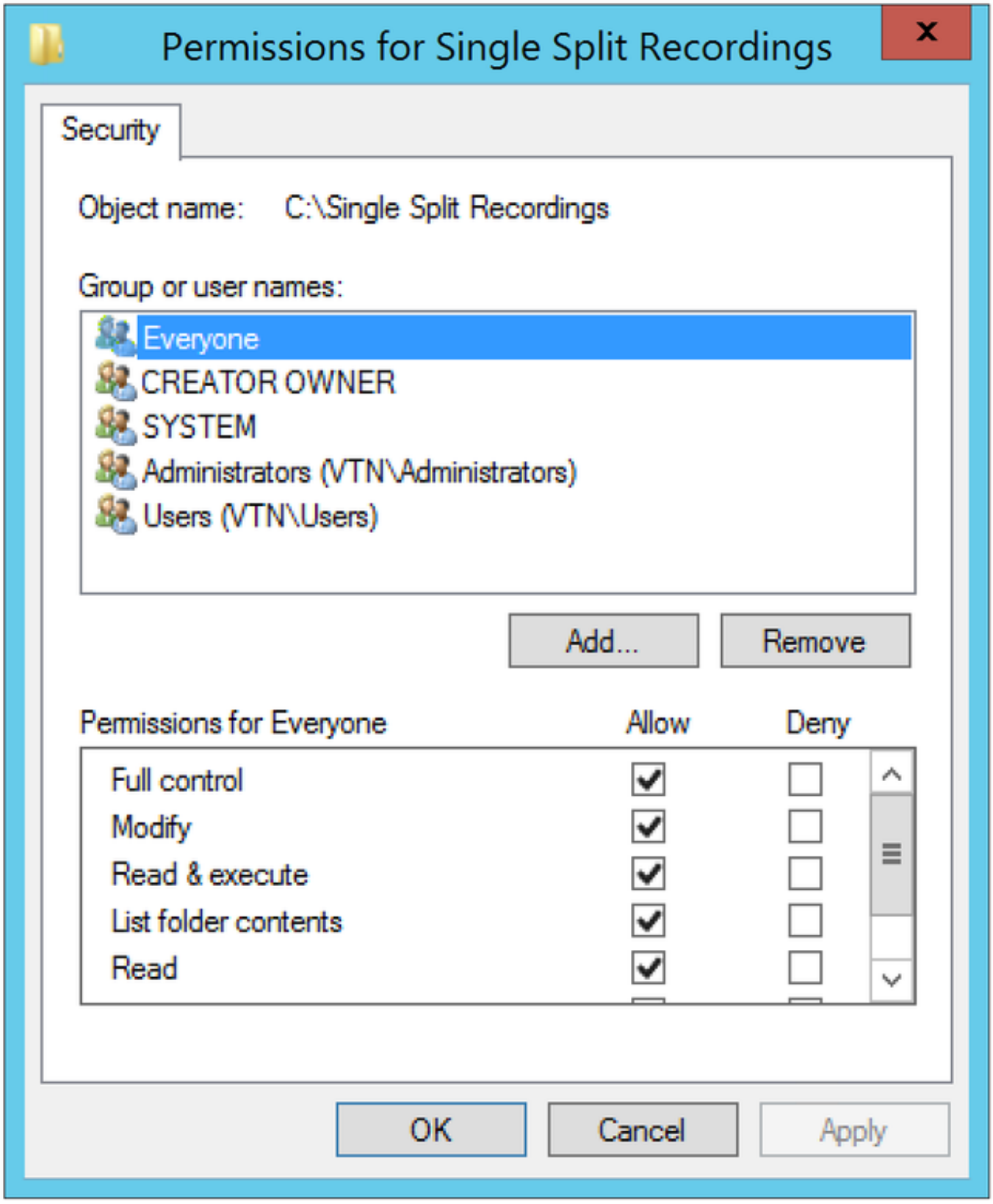
r. Modifier **Type d'accès** par **Pas d'accès**

art. Sélectionner **OK** pour fermer la fenêtre autorisations

t. Sélectionner **OK** pour revenir à la fenêtre Propriétés du dossier

u. Sélectionner **Sécurité**

> **Note**: Le groupe **Tout le monde** doit avoir un accès complet au dossier. S'il ne figure pas dans la liste, sélectionnez **Modifier** pour ouvrir l'éditeur Autorisations. Sélectionnez **Ajouter** pour ajouter un utilisateur, et dans le champ de noms, saisissez **Tout le monde** et sélectionnez OK. Sélectionnez **Tout le monde** dans la liste, cochez la case **Contrôle total** et sélectionnez **OK**. Sélectionnez **OK** à nouveau pour fermer les propriétés. Si elle est correctement configurée, elle ressemble à l'image suivante :



Étape 2. Configurer et activer l'enregistreur sur le serveur d'enregistreurs

a. Configurez l'enregistreur pour écouter sur les interfaces de votre choix à l'aide de la commande suivante :

enregistreur écoute <liste blanche interface[:port]>

b. Si l'enregistreur se trouve sur la CB locale, l'interface doit être définie sur “ ” de bouclage, donc

utilisez cette commande :

écoute enregistreuse :8443

c. S'il doit écouter sur une interface spécifique, disons “ un ”, utilisez ceci :

enregistreur écoute a:8443

> **Note**: Si vous configurez l'enregistreur sur un noeud de CB en cluster, l'interface doit être l'interface d'écoute locale du noeud sur lequel l'enregistreur est configuré.

d. Définissez le fichier de certificat à utiliser par l'enregistreur. Vous pouvez utiliser un certificat qui existe déjà et un fichier de clé privée utilisé par la CB, par exemple.

recorder certs <keyfile> <certificat file>

e. Ajoutez le certificat CB au magasin d'approbation de l'enregistreur à l'aide de la commande :

confiance de l'enregistreur <bundle crt>

L'ensemble crt doit contenir le certificat utilisé par la BC, si différent. Dans un cluster, il doit contenir les certificats de chaque CB du cluster.

f. Spécifiez le nom d'hôte ou l'adresse IP du NFS et le répertoire sur le NFS pour stocker les enregistrements :

enregistreur nfs <nom d'hôte/IP> : <répertoire>

> **Note**: L'enregistreur ne s'authentifie pas auprès du NFS, mais il est important que le serveur d'enregistreurs dispose d'un accès en lecture/écriture au répertoire NFS.

g. Activez l'enregistreur à l'aide de la commande suivante :

enregistreur enable

Étape 3. Créer un utilisateur API sur la CB

Créez un utilisateur d'API sur la CB, ceci est nécessaire pour d'autres configurations à l'aide de la fonction API :

Créez l'utilisateur en procédant comme suit :

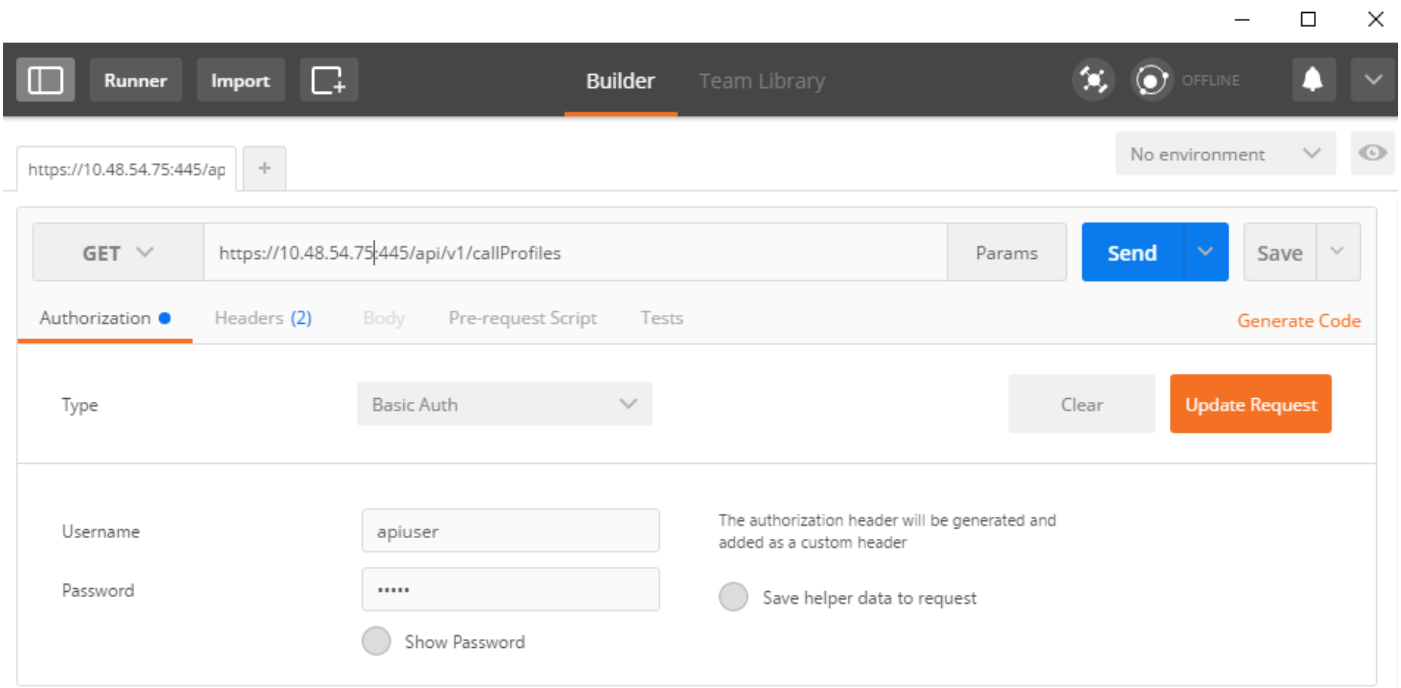
a. Connectez-vous via Secure Shell (SSH) ou console à la CB à l'aide des informations d'identification d'administrateur.

b. L'utilisateur ajoute **<nom d'utilisateur>** api, puis appuie sur la touche **Retour** et saisissez le mot de passe suivi de la clé **de retour**.

Étape 4. Ajoutez l'enregistreur à la CB à l'aide de l'API

1. Télécharger et installer Postman à partir d'ici

2. Saisissez l'URL d'accès à l'API dans la barre d'adresses, par exemple : **https://<Callbridge_IP>:445/api/v1/<entity>**. Ensuite, définissez l'authentification, le nom d'utilisateur et le mot de passe de l'étape 3, sous Autorisation avec **authentification de base** comme type



> **Note**: Cela suppose qu'aucun enregistreur ou profil d'appel n'est actuellement configuré sur la CB. Sinon, vous pouvez modifier un enregistreur existant et/ou callProfile à l'aide de la méthode PUT.

3. Ajouter l'enregistreur à la CB avec l'API

a. Envoyer un POST vide avec https://<Callbridge_IP>:445/api/v1/enregistreurs

b. Envoyez une requête GET avec la même URL en (a), copiez l'ID de l'enregistreur, sans les devis dans le Bloc-notes

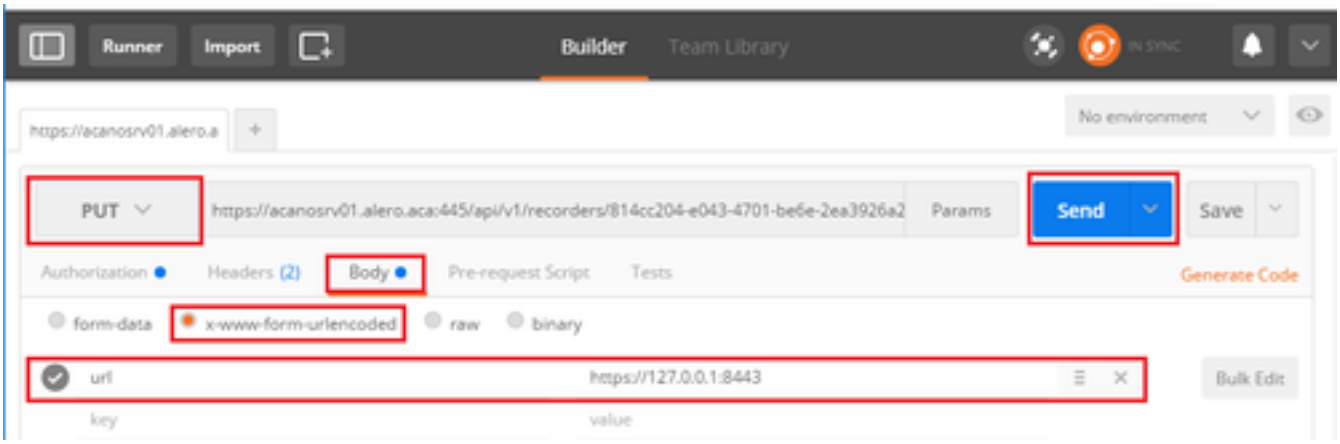
c. Définissez l'URL de l'enregistreur en envoyant un PUT avec https://<Callbridge_IP>:445/api/v1/recorders/<enregisterid> et ajoutez-le dans CORPS avant d'exécuter le PUT :

url=https://127.0.0.1:8443 (si l'enregistreur se trouve sur la BC locale)

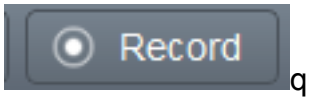
ou

url=https://<Adresse IP de l'enregistreur>:8443 (si l'enregistreur n'est pas sur la BC locale)

Exemple :



Note: **dtmfProfile**, **callProfile** et **callLegProfile** sont particulièrement importants pour les points de terminaison SIP qui rejoignent une conférence cospace. Ils permettent au point de terminaison de démarrer/arrêter l'enregistrement d'un appel en provenance ou à destination du coespace.

Àpartir de CMA 1.9.3 et CMS 2.0.1, les tonalités DTMF ne sont pas requises maintenant qu'il existe 

qui est ajouté au client lorsque l'enregistreur est présent sur ou connu du pont d'appel auquel le client est connecté. Le bouton d'enregistrement a également été ajouté à WebRTC à partir de CMS 2.3.

4. Créer un callProfile

a. Envoyer un POST vide avec **https://<Callbridge_IP>:445/api/v1/callProfiles**

b. Envoyer une requête GET avec la même URL en (a), copier l'ID callProfile, sans les devis vers le Bloc-notes

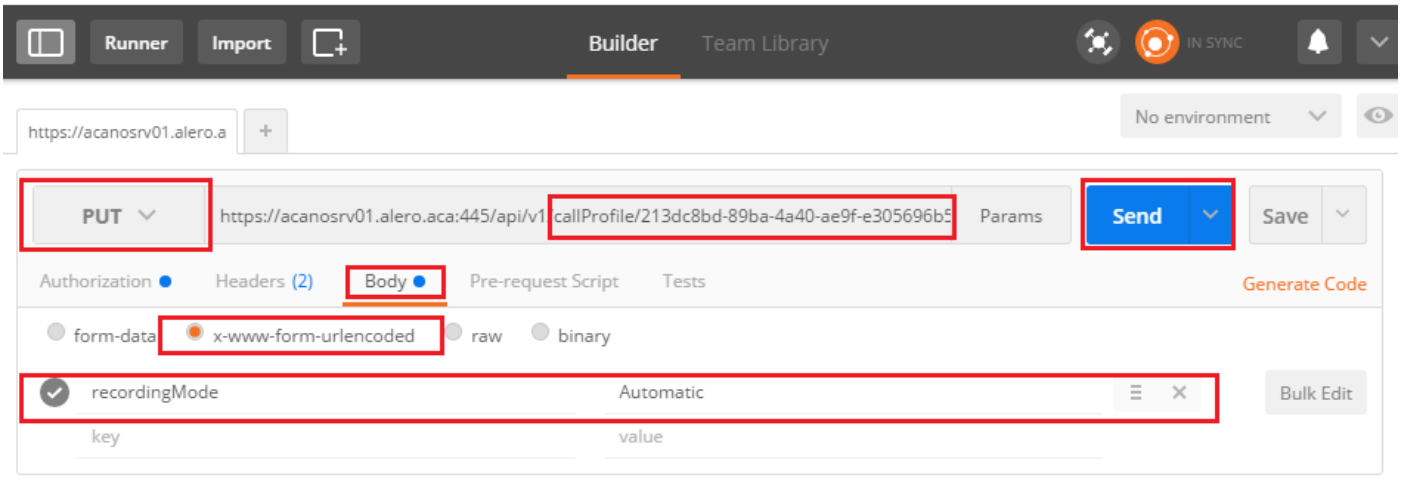
c. Définissez le mode enregistrement sur callProfile en envoyant un PUT avec **https://<Callbridge_IP>:445/api/v1/callProfiles/<call profile ID>** et ajoutez le dans BODY avant d'exécuter le PUT.

loggingMode=Manual (si vous voulez que les appelants commencent l'enregistrement à l'aide d'entrées DTMF)

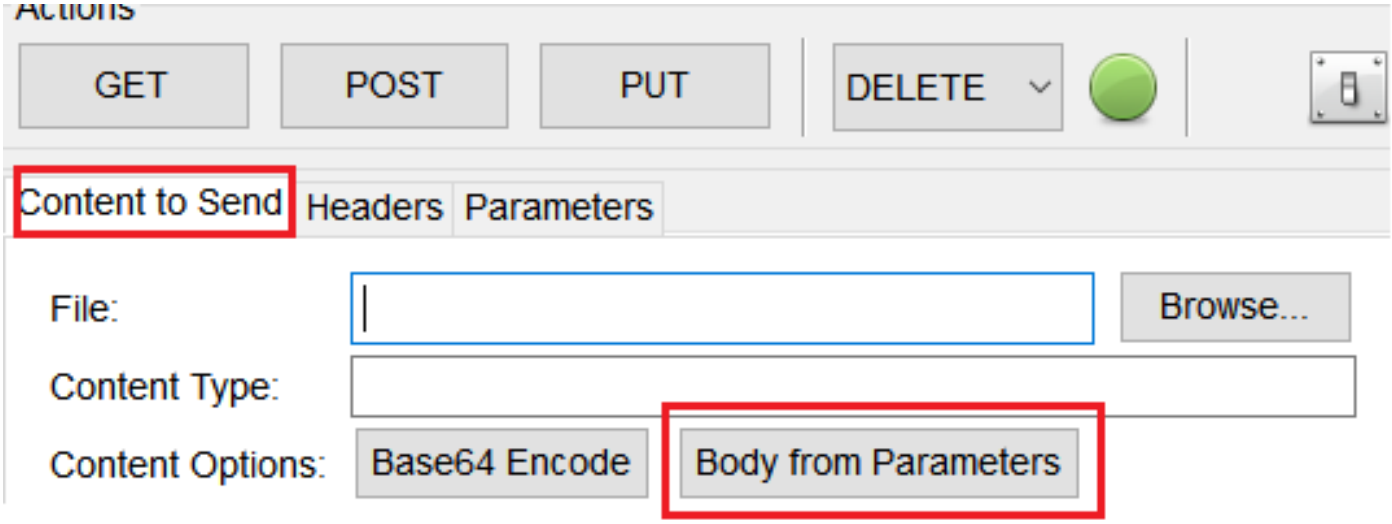
ou

loggingMode=Automatique (si l'enregistrement doit être démarré automatiquement lors du lancement des appels)

Exemple :



Note: Si vous utilisez POSTER à partir de firefox, vous devez sélectionner **Contenu à envoyer** puis sélectionner **Corps à partir des paramètres** avant d'envoyer le PUT/POST, de cette façon il est compilé dans le(s) code(s) que la CB peut comprendre. Comme dans l'image suivante :



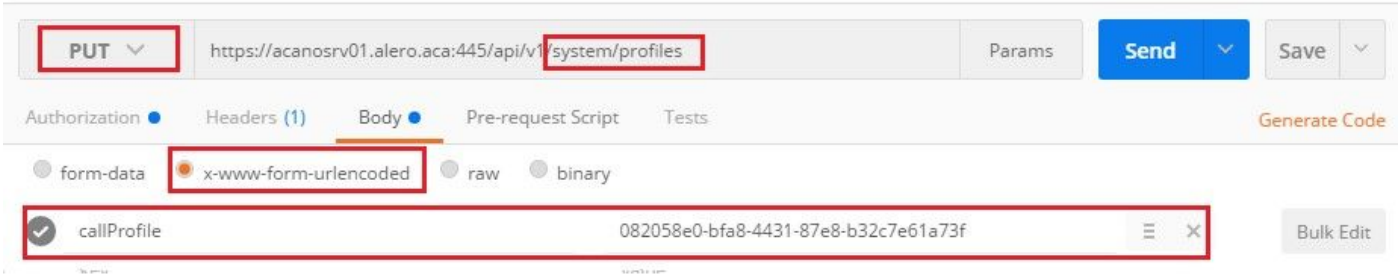
5. Ajouter un profil d'appel aux profils système

Le callProfile définit si les appels peuvent être des enregistrements et s'ils peuvent être effectués avec ou sans intervention de l'utilisateur.

Envoyer un PUT avec https://<Callbridge_IP>:445/api/v1/system/profile après avoir ajouté le callProfile dans BODY

callProfile=<ID du profil d'appel>

Exemple :

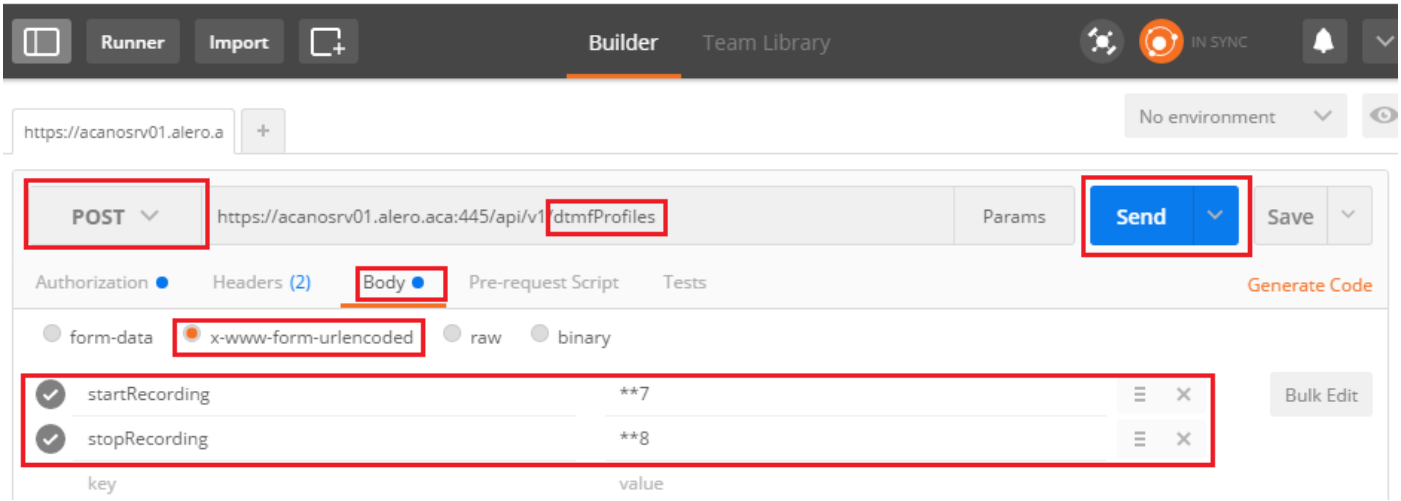


Si le mode enregistrement est défini sur Manual, vous devez définir un profil DTMF pour définir comment les utilisateurs peuvent démarrer et arrêter des enregistrements à l'aide de tonalités DTMF.

6. Créer le profil DTMF

a. Envoyez une publication avec https://<Callbridge_IP> :445/api/v1/dtmfProfiles après avoir défini les paramètres startRecording=**7 et stopRecording=**8 (par exemple) dans BODY en tant que startRecording=**7&stopRecording=**8.

Exemple :



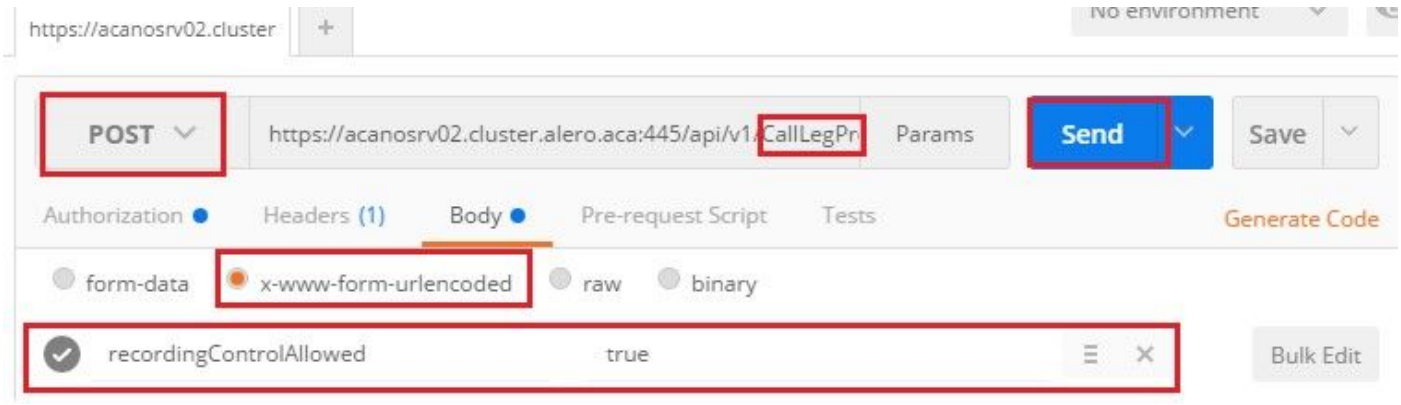
b. Envoyez un GET pour voir le nouveau profil DTMF, puis copiez l'ID sans les devis sur le bloc-notes.

7. Créer un profil CallLeg

CallLegProfiles détermine le comportement en appel. Dans ce cas, il détermine si un appel peut être enregistré.
Créez un profil de segment d'appel comme suit :

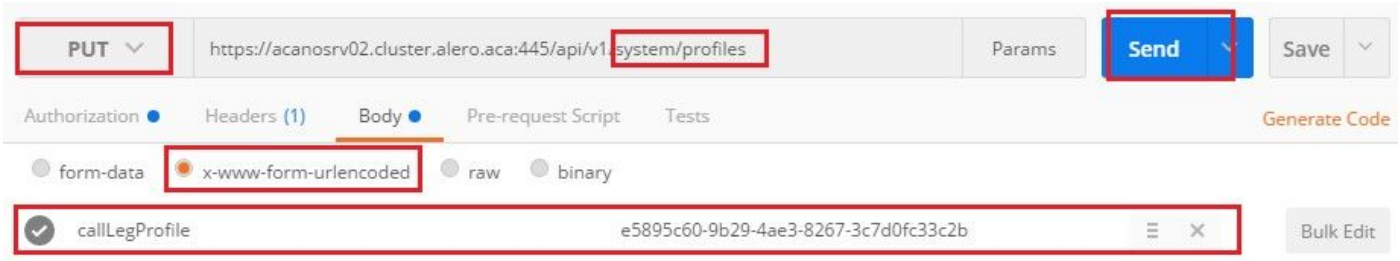
a. Envoyer un message avec https://<Callbridge_IP>:445/api/v1/CallLegProfiles après avoir ajouté la propriété enregistrementControlAllowed=true dans le CORPS :

Exemple :



b. Appliquez CallLegProfile en envoyant un PUT avec https://<Callbridge_IP>:445/api/v1/system/profile et en ajoutant callLegProfile=<callLegProfile_ID> dans le CORPS :

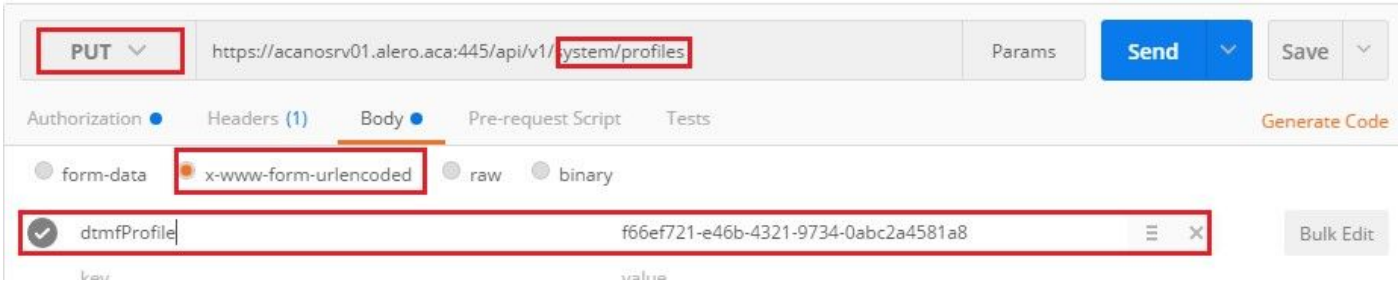
Exemple :



8. Appliquer le profil DTMF :

Envoyer un PUT avec https://<Callbridge_IP>:445/api/v1/system/profile après avoir ajouté le dtmfProfile dans BODY dtmfProfile=<dfmt Profile ID>

Exemple :



Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement

1. Une fois configuré, vérifiez son état à l'aide de ces commandes, vous pouvez obtenir une sortie similaire à celle de l'image suivante

enregistreur

CB autonome locale :

```
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
```

Ou si CB en cluster :

```
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. Envoyer un GET pour afficher le profil système, vous devez voir le **callProfile**, **CallLegProfile** et **dtmfProfile** (en supposant que tous ces éléments ont été configurés) dans le résultat avec

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

Exemple :

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

3. Pour vérifier ce qui a été configuré sur CallProfile, utilisez ceci sur l'API

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

Ceci montre que les méthodes d'enregistrement ont été définies, Automatique ou Manuelle, comme indiqué :

```
<?xml version="1.0"?>
<callProfile id="af73f145-829b-42ed-898d-f111f6259626">
    <recordingMode>automatic</recordingMode>
</callProfile>
```

4. Pour vérifier ce qui est configuré sur CallLegProfile, utilisez cette API

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

Exemple de rapport :

```
1  <?xml version="1.0"?>
2  <callLegProfile id="9591bd29-dc78-4656-bab1-328b2fd505fe">
3      <recordingControlAllowed>true</recordingControlAllowed>
4  </callLegProfile>
```

5. Pour vérifier ce qui a été configuré sur le profil DTMF, utilisez cette option sur l'API

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

Ceci montre que les méthodes d'enregistrement ont été définies, Automatique ou Manuelle, comme indiqué :

```
<?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>
```

Note: Les profils DTMF ne fonctionnent pas dans les appels point à point. Vous ne pouvez donc utiliser l'enregistrement manuel que dans un espace.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Pour afficher ce qui est consigné par rapport à l'enregistreur, exécutez la commande suivante :

suivi syslog

Le résultat affiché est similaire à celui-ci :

```
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
```

Dans cet exemple, acanosrv05 est le serveur qui héberge l'enregistreur et les autres noeuds CB qui y sont connectés sont 10.48.54.75 et 10.48.54.76.

Ceci montre que la CB distante se connecte et s'authentifie correctement avec l'enregistreur.

Si l'enregistreur est local à la CB, la connexion proviendra de l'adresse IP de bouclage :

```
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
```

> **Note**: La plupart des journaux liés aux processus de l'enregistreur sont affichés dans le syslog en tant que recorder-proxy, ce qui indique où l'enregistreur peut échouer.

Les autres syslogs sont affichés comme suit pour l'enregistreur :

Dans ce cas, un périphérique d'enregistrement est trouvé et l'enregistrement démarre automatiquement :

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

Si l'enregistrement échoue, vérifiez si un périphérique d'enregistrement est trouvé :

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

Si vous voyez un tel avertissement, vérifiez le certificat dans l'approbation de l'enregistreur pour vous assurer qu'il est le bon utilisé pour configurer la CB.

Vérifiez le syslog pour voir si le stockage NFS est monté :

- Si le stockage NFS n'est pas monté, « Échec du montage du stockage NFS » s'affiche.
- Vérifiez et assurez-vous que le dossier NFS défini sur le serveur d'enregistreurs : /Folder-name est identique à celui configuré sur le stockage NFS

Exécutez l'API pour vérifier les alarmes liées à l'enregistreur :

- **https://<callBridge_IP>api/v1/system/alarms**
- Si l'espace disque est insuffisant, « RecorderLowDiskSpace » s'affiche
- Vérifiez ensuite que le stockage NFS référencé par l'enregistreur a suffisamment d'espace disque

Informations connexes

- Support et documentation techniques - Cisco Systems