

Configurez l'enregistreur dans la passerelle d'appel CMS/Acano

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Déploiements](#)

[Déploiements pris en charge](#)

[L'autre installation](#)

[Configurez](#)

[Vérifiez et dépannez](#)

Introduction

Ce document décrit les étapes de configuration requises pour installer l'enregistreur sur Cisco rencontrant la passerelle d'appel du serveur (CMS) (CB).

L'enregistreur est fourni par la version 1.9 du serveur d'Acano. L'enregistreur fournit le capability des téléconférences et de l'économie d'enregistrement les enregistrements sur un stockage de documents de Systèmes de fichiers en réseau (NFS).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

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

1. CMS 1.9 ou en haut
2. Facteur de Google Chrome
3. Interface de programmation CMS (API)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dedans ici démarrés avec des configurations (par défaut) effacées. Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

1. L'enregistreur se comporte comme un client extensible de Protocol de Messagerie et de présence (XMPP), ainsi le serveur XMPP doit être activé sur le serveur qui héberge la passerelle d'appel.

2. Permis d'enregistreur, qui doit être sur les CB et pas le serveur d'enregistreur, si exécutant des versions avant CMS 2.X, plus d'informations ici <https://kb.acano.com/content/23/280/en/how-does-licensing-work-on-the-acano-solution.html>.

3. Répertoire de Systèmes de fichiers en réseau (NFS), qui peut être installé sur des Windows Server ou le Linux.

Pour des Windows Server, suivez les étapes dans ce lien : [https://technet.microsoft.com/en-us/library/jj574143\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj574143(v=ws.11).aspx).

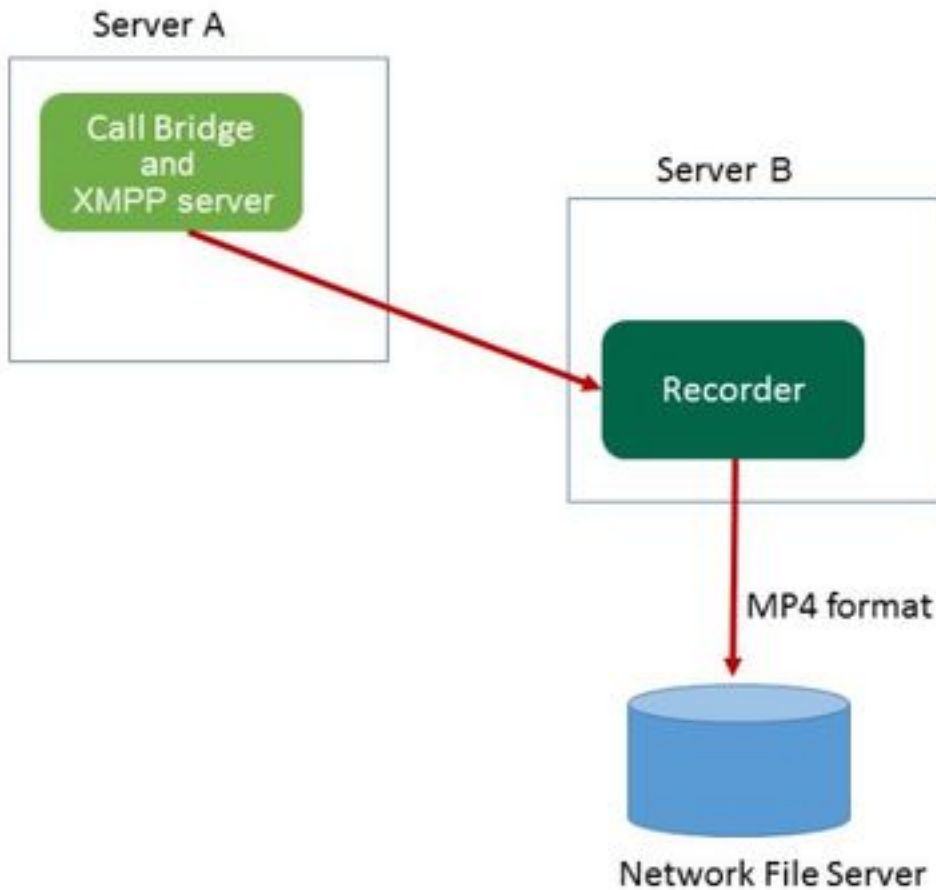
Pour le Linux, suivez les étapes dans ce lien : <https://help.ubuntu.com/lts/serverguide/network-file-system.html>.

Note: Pour le NFS qui exécute sur les Windows Server 2008 R2 là un correctif pour la question d'autorisation : <https://support.microsoft.com/en-us/kb/2485529>.

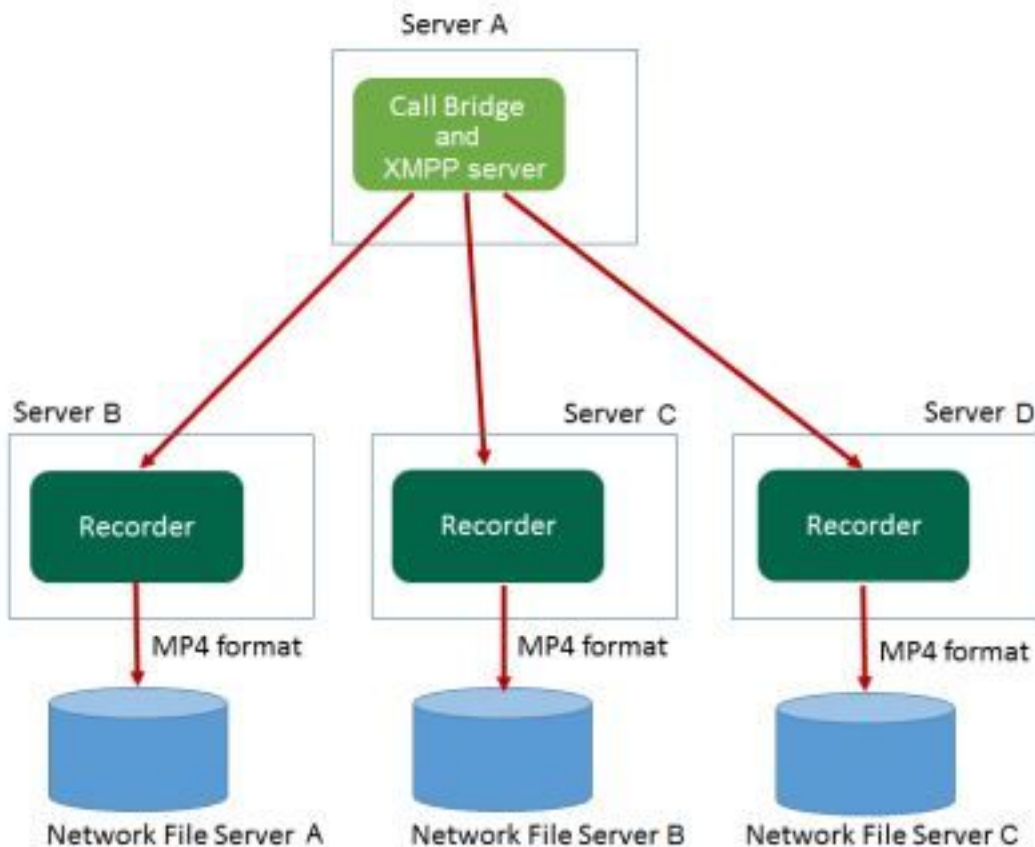
Déploiements

Déploiements pris en charge

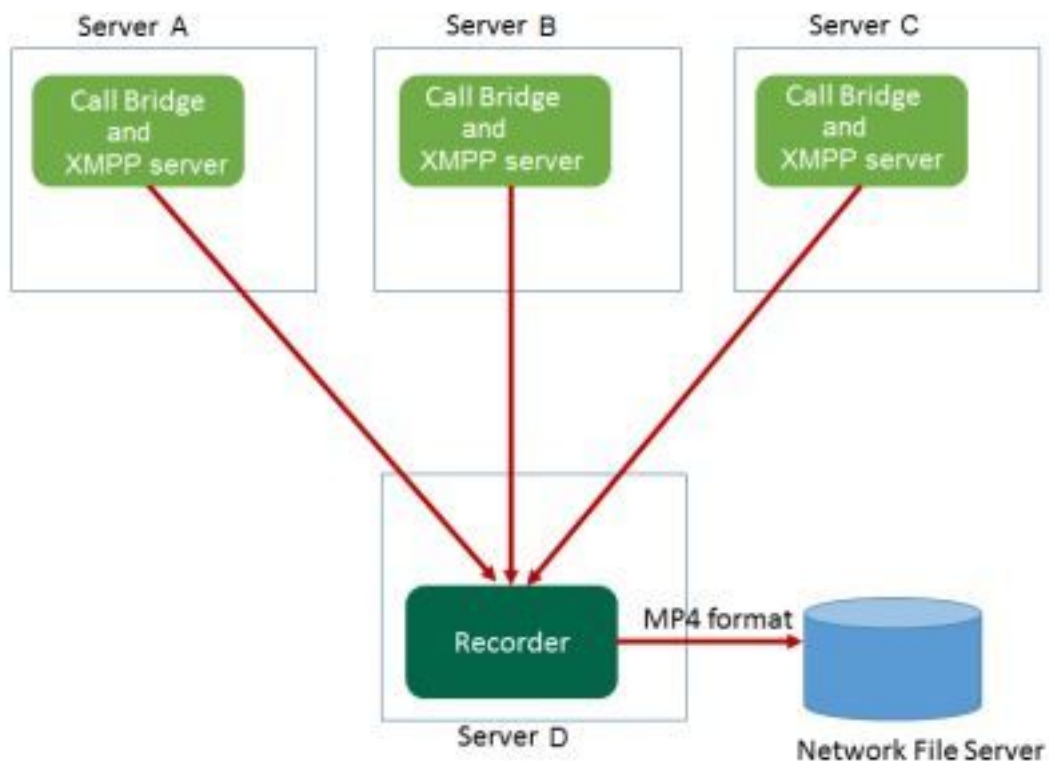
1. L'enregistreur devrait être hébergé sur un serveur d'Acano qui est distant au serveur qui héberge les CB suivant les indications de cette figure :



2. Le déploiement redondant de l'enregistreur est également pris en charge. Si la Redondance est installée, les enregistrements sont chargement équilibré entre tous les périphériques d'enregistrement (serveurs). Ceci signifie que chaque CB utilisera chaque enregistreur disponible, comme cette figure affiche :

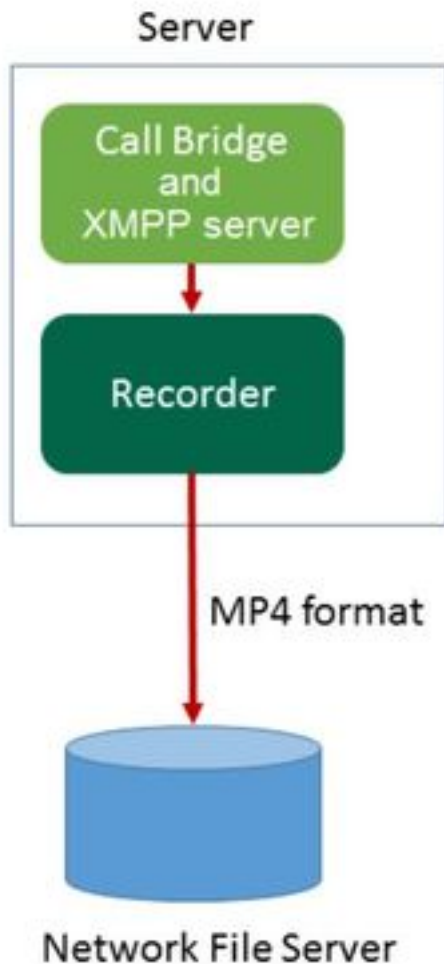


3. Le même s'applique dans l'opposé, quand il y a de CBS de multiple. Tout le CBS utilisera l'enregistreur disponible à eux, comme cette figure affiche :



L'autre installation

L'enregistreur peut également être hébergé sur le même serveur que les CB, mais ceci devrait seulement être utilisé pour tester ou les déploiements très petits, voient la figure. L'inconvénient ici est que vous pouvez seulement pouvoir faire 1 -2 enregistrements simultaneus :



Configurez

Partie : Sur le serveur d'enregistreur :

a. Configurez l'enregistreur pour écouter sur les interfaces de votre choix avec cette commande :

l'enregistreur écoute <interface [: whitelist> de port]

b. Si l'enregistreur est sur les CB locaux, l'interface doit être le positionnement au « bouclage », ainsi utilisez cette commande :

l'enregistreur écoute lo:8443

c. S'il est d'écouter sur une interface spécifique, permettez-nous disent « a », alors utilisent ceci :

l'enregistreur écoute a:8443

NOTE: Si vous configurez l'enregistreur sur un noeud des CB groupés, l'interface devrait être l'interface de écoute locale du noeud sur lequel l'enregistreur est configuré.

d. Placez le fichier du certificat à utiliser par l'enregistreur. Vous pouvez utiliser un certificat qui existe déjà et fichier principal privé utilisé par les CB, par exemple.

<certificatefile> de <keyfile> de CERT d'enregistreur

e. Ajoutez le certificat de CB à la mémoire de confiance d'enregistreur utilisant la commande :

<crt-bundle> de confiance d'enregistreur

Le tube-paquet devrait contenir le certificat utilisé par les CB, si différent. Si dans une batterie, ceci doit contenir les Certificats de chaque CB dans la batterie.

f. Spécifiez l'adresse Internet ou l'adresse IP du NFS, et le répertoire sur le NFS pour enregistrer les enregistrements :

NFS <hostname/IP> d'enregistreur : <directory>

NOTE: L'enregistreur n'authentifie pas au NFS mais il est important que le serveur d'enregistreur ait accès lecture/écriture au répertoire NFS.

g. Activez l'enregistreur, avec l'utilisation de la commande :

enable d'enregistreur

Partie : Sur les CB :

Créez un utilisateur API sur les CB, ceci est exigé pour d'autres configurations utilisant la fonction API :

Créez l'utilisateur avec ces étapes :

a. Connectez par l'intermédiaire du Protocole Secure Shell (SSH) ou consolez aux CB avec l'utilisation des qualifications d'admin.

b. L'utilisateur ajoutent le <username> api, puis appuient sur la touche **de retour** et entrent le mot de passe suivi de la clé **de retour**.

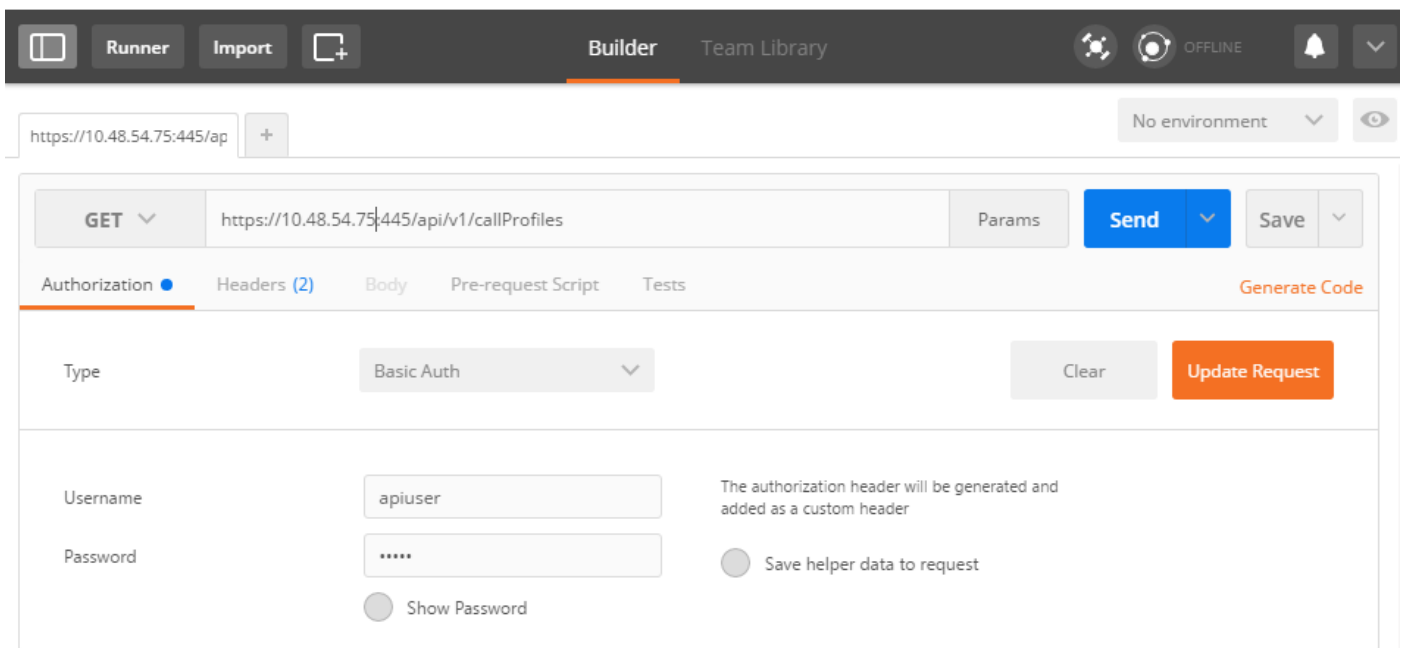
Partie 3 : Utilisant l'API :

1. Téléchargez et installez le facteur de ; <https://chrome.google.com/webstore/detail/postman/fhbjgbiflinjbdgggehcdcbncdddop?hl=en>

2. Écrivez l'URL d'accès API dans la barre d'adresses, par exemple :

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

Puis, positionnement dans l'authentification, le nom d'utilisateur et mot de passe de la partie, sous l'autorisation avec **authentique de base** en tant que type :



NOTE: Ceci suppose qu'il n'y a actuellement aucun enregistreur ou callProfile configuré sur les CB. Autrement vous pouvez modifier un enregistreur qui existe et/ou callProfile avec l'utilisation de la méthode MISE.

3. Ajoutez l'enregistreur aux CB avec l'API :

a. Envoyez un POST vide avec https://<Callbridge_IP>:445/api/v1/recorders

b. Envoyez un OBTENIR avec le même URL en (a), copiez l'ID d'enregistreur, sans devis sur Notepad

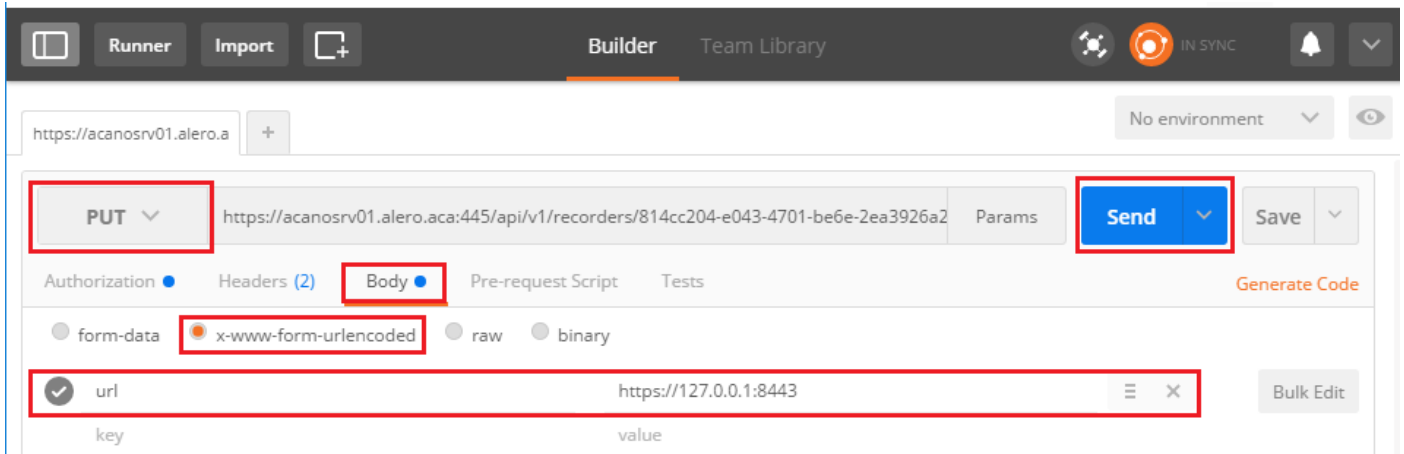
c. Placez l'URL de l'enregistreur en envoyant MIS avec https://<Callbridge_IP>:445/api/v1/recorders/<recorderid> et ajoutez ceci dans le CORPS avant que vous exécutiez MIS :

url= <https://127.0.0.1:8443> (si l'enregistreur est sur les CB locaux)

ou

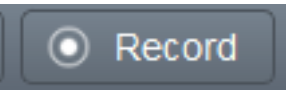
url= https:// < adresse IP de recorder>:8443 (si l'enregistreur n'est pas sur les CB locaux)

Exemple :



Note: *dtmfProfile*, *callProfile* et *callLegProfile* sont particulièrement importants pour les points finaux de SIP qui joignent une conférence de **cospace**. Ils permettent au point final pour pouvoir ont to start/stop l'enregistrement d'un appel à/de le **cospace**.

Comme de CMA 1.9.3 et de CMS 2.0.1, les tonalités DTMF ne sont pas exigées maintenant là

est  le bouton qui est ajouté au client quand l'enregistreur est allumé présent ou connu du callbridge auquel le client est connecté. Le bouton d'enregistrement a été aussi bien ajouté à WebRTC de CMS 2.3.

4. Créez un callProfile :

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

b. Envoyez un OBTENIR avec le même URL en (a), copiez l'ID callProfile, sans devis sur Notepad

c. Placez le recordingMode sur le callProfile en envoyant MIS avec le profil ID>

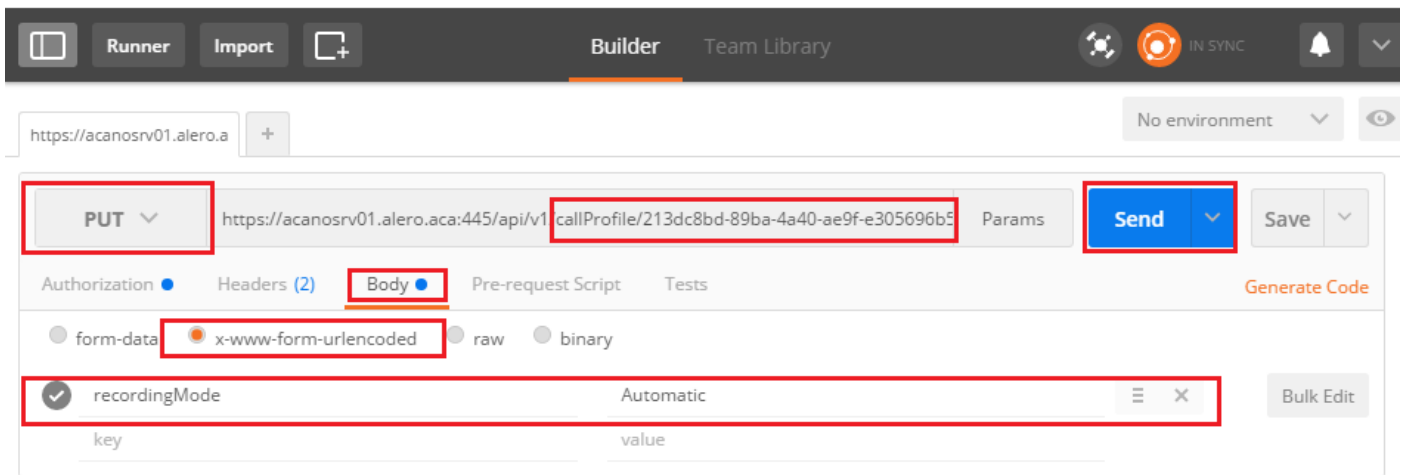
`https://<Callbridge_IP>:445/api/v1/callProfiles/<call` et ajoutez dans le CORPS avant que vous exécutiez MIS.

recordingMode=Manual (si vous voulez que les appelants commencent l'enregistrement utilisant des entrées DTMF)

ou

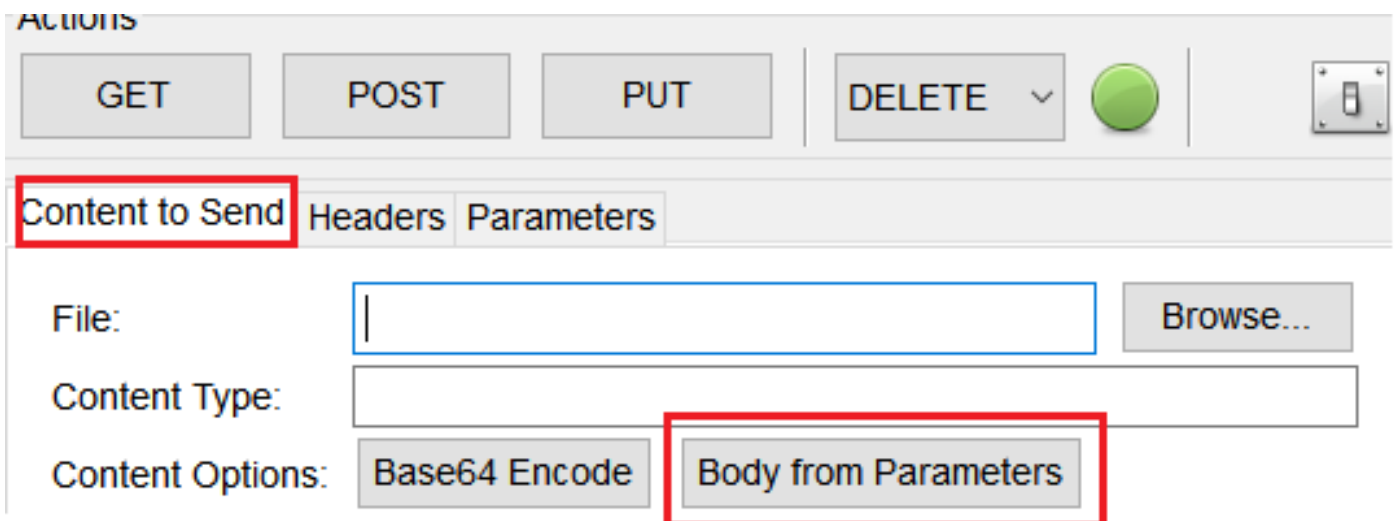
recordingMode=Automatic (si enregistrant commencez automatiquement quand des appels sont lancés)

Exemple :



NOTE: Si vous utilisez le POSTER du firefox, vous devez cliquer sur en fonction « satisfait pour envoyer » sélectionnez alors le « corps des paramètres »

avant d'envoyer le PUT/POST, de cette façon qu'elle a compilée dans les codes que les CB peuvent comprendre.



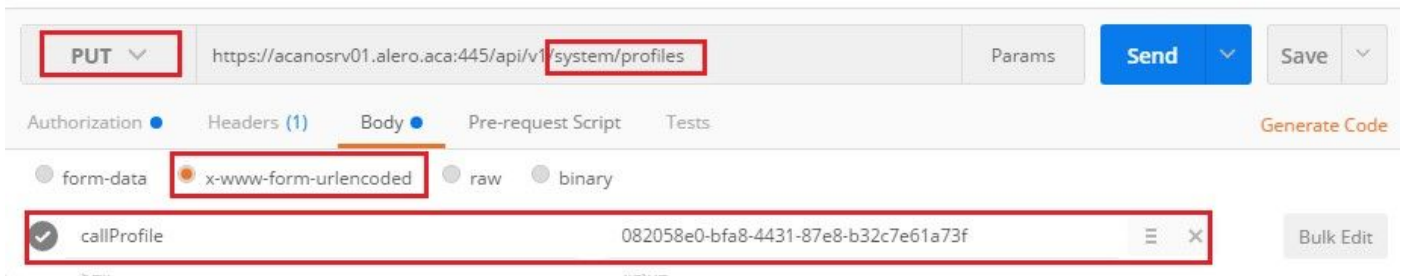
5. Ajoutez le profil d'appel aux profils de système :

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

Envoyez MIS avec https://<Callbridge_IP>:445/api/v1/system/profiles après que vous ajoutiez le callProfile dans le CORPS

profil ID> de callProfile=<call

Exemple :

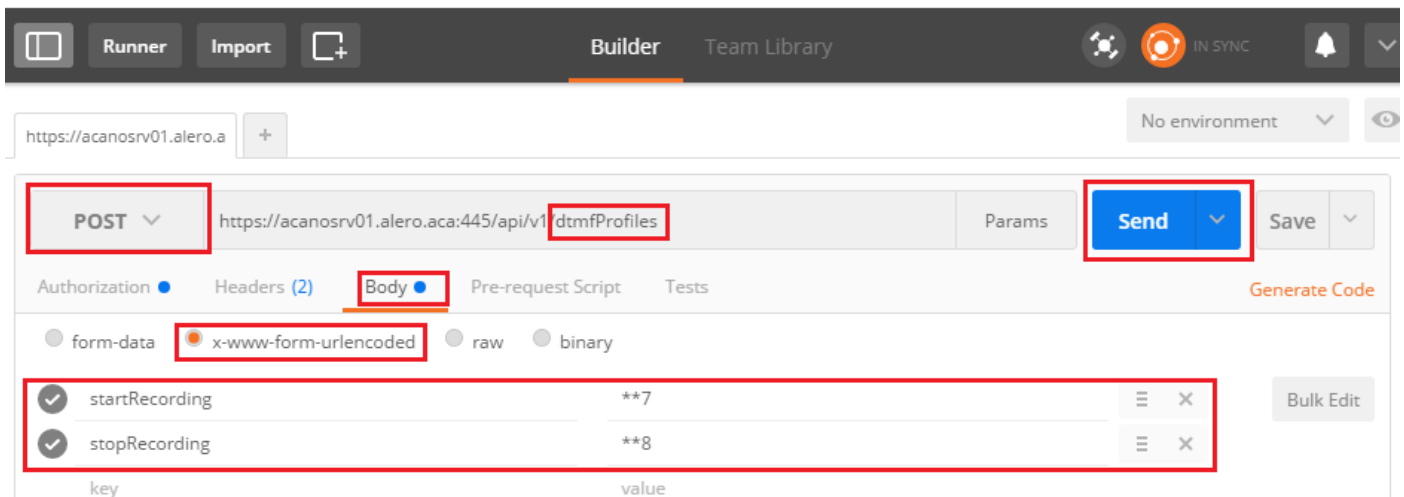


Si le recordingMode est placé au manuel, vous devez placer un profil DTMF pour définir comment les utilisateurs peuvent commencer et arrêter des enregistrements utilisant des tonalités DTMF.

6. Créez le profil DTMF :

a. Envoyez un courrier avec [https:// <Callbridge IP>:445/api/v1/dtmfProfiles](https://<Callbridge IP>:445/api/v1/dtmfProfiles) après que vous ayez placé le startRecording=**7 et le stopRecording=**8 (par exemple) dans le CORPS comme startRecording=**7&stopRecording=**8.

Exemple :



b. Envoyez un OBTENIR pour voir le nouveau profil DTMF, puis copiez l'ID sans devis sur le Notepad.

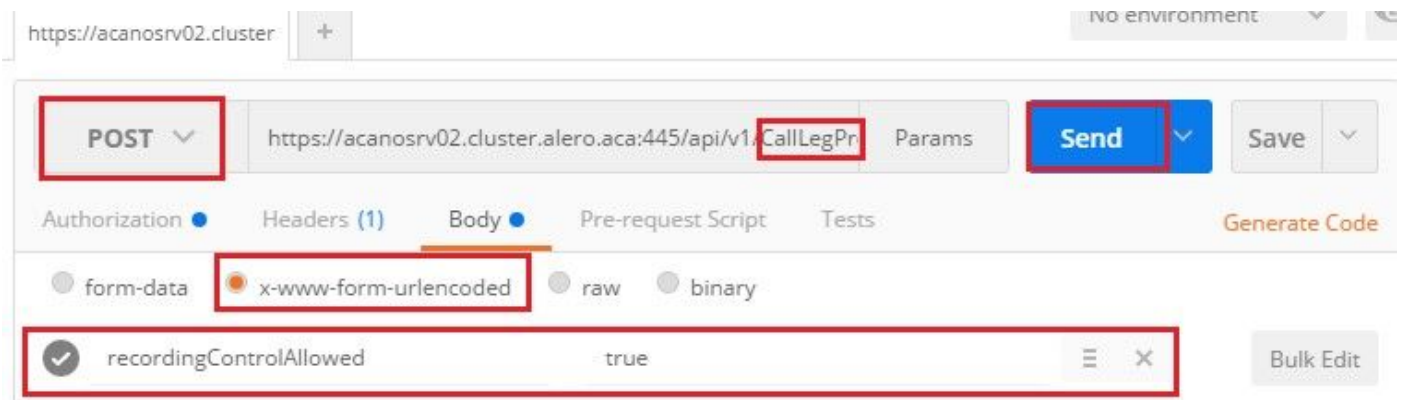
7. Créez le profil de CallLeg :

CallLegProfiles détermine le comportement de dans-appel. Dans ce cas il détermine si des appels peuvent être enregistrés.

Créez un profil de tronçon d'appel comme suit :

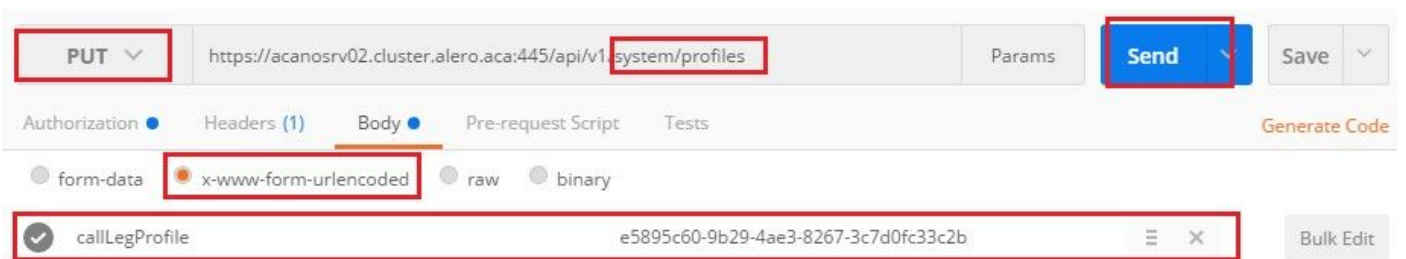
a. Envoyez un courrier avec <https://<Callbridge IP>:445/api/v1/CallLegProfiles> après que vous ayez ajouté le recordingControlAllowed=true dans le CORPS :

Exemple :



b. Appliquez le CallLegProfile, en envoyant MIS avec <https://<Callbridge IP>:445/api/v1/system/profiles> et en ajoutant le callLegProfile=<callLegProfile_ID> dans le CORPS :

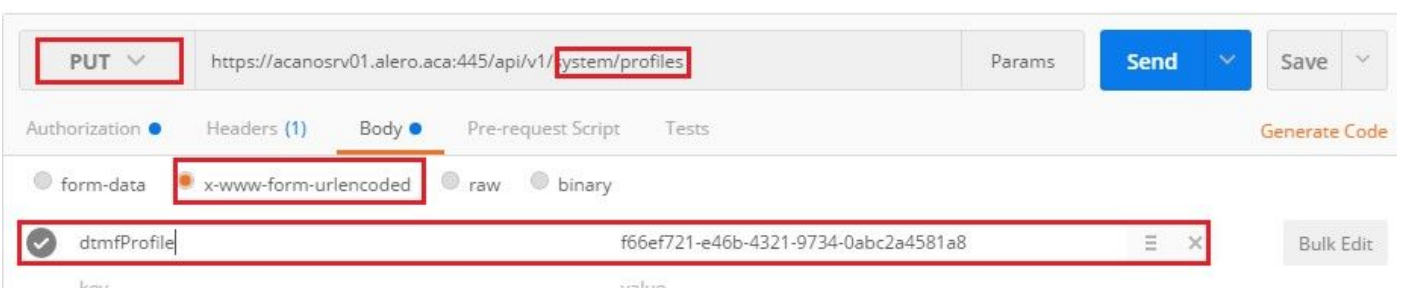
Exemple :



8. Appliquez le profil DTMF :

Envoyez MIS avec <https://<Callbridge IP>:445/api/v1/system/profiles> après que vous ajoutiez le dtmfProfile dans le profil ID> de dtmfProfile=<dfmt de CORPS

Exemple :



Vérifiez et dépannez

1. Une fois que configuré, vérifiez son état avec ces commandes, il devrait être semblable à cette sortie :

enregistreur

CB autonomes locaux :

```
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 groupés :

```
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. Envoyez un OBTENIR pour visualiser le profil de système, vous devrait voir le callProfile, le CallLegProfile et le dtmfProfile dans le résultat avec :

[https:// <Callbridge_IP>:445/api/v1/system/profiles](https://<Callbridge_IP>:445/api/v1/system/profiles)

Exemple :

```
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. Pour vérifier ce qui est configuré sur le CallProfile, utilisez ceci sur l'API :

[https:// <Callbridge_IP>:445/api/v1/callProfiles/<callProfile_ID>](https://<Callbridge_IP>:445/api/v1/callProfiles/<callProfile_ID>)

Ceci affiche que des méthodes d'enregistrement a été placé, automatique ou manuel, comme affiché :

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

4. Pour vérifier ce qui est configuré sur le CallLegProfile, utilisez cet API :

[https:// <Callbridge_IP>:445/api/v1/callLegProfiles/<callLegProfile_ID>](https://<Callbridge_IP>:445/api/v1/callLegProfiles/<callLegProfile_ID>)

Exemple de sortie :

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

5. Pour vérifier ce qui est configuré sur le profil DTMF, utilisez ceci sur l'API :

[https:// <Callbridge_IP>:445/api/v1/dtmfProfiles/<dtmfProfile_ID>](https://<Callbridge_IP>:445/api/v1/dtmfProfiles/<dtmfProfile_ID>)

Ceci prouve que l'enregistrement des méthodes a été placé, automatique ou manuel, comme affiché :

```
<?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 des appels point par point, ainsi vous pouvez seulement utiliser l'enregistrement manuel dans un espace.

6. Pour afficher ce qui est enregistré en ce qui concerne l'enregistreur, exécutez la commande :

le Syslog suivent

Vous devriez voir quelque chose semblable à cette sortie :

20 juin 20:38:49 kern.info acanosrv05 recorder-proxy[1] : 2016/06/20 connexion de 20:38:49 de 10.48.54.75:39439 :

Authentification réussie

20 juin 20:38:49 kern.info acanosrv05 recorder-proxy[1] : 2016/06/20 connexion de 20:38:49 de 10.48.54.75:39439 :

Connexion terminée

20 juin 20:38:53 kern.info acanosrv05 recorder-proxy[1] : 2016/06/20 connexion de 20:38:53 de 10.48.54.76:35141 :

Authentification réussie

20 juin 20:38:53 kern.info acanosrv05 recorder-proxy[1] : 2016/06/20 connexion de 20:38:53 de 10.48.54.76:35141 :

Connexion terminée

Dans cet exemple acanosrv05 est le serveur accueillant l'enregistreur et les autres Noeuds de CB

se connectant à lui sont 10.48.54.75 et 10.48.54.76.

Cette exposition que les CB distants sont correctement se connectants et authentifiants avec l'enregistreur.

Si l'enregistreur est local aux CB, alors la connexion proviendrait l'IP de bouclage :

20 juin 20:40:52 kern.info acanosrv01 recorder-proxy[1] : 2016/06/20 connexion de 20:40:52 de 127.0.0.1:45380 :

Authentification réussie

20 juin 20:40:52 kern.info acanosrv01 recorder-proxy[1] : 2016/06/20 connexion de 20:40:52 de 127.0.0.1:45380 :

Connexion terminée

Note: La plupart des logs liés aux processus d'enregistreur sont affichés dans le Syslog comme enregistreur-**proxy**, ceux-ci donnent une indication où l'enregistreur pourrait manquer.

D'autres Syslog sont affichés comme suit pour l'enregistreur :

Dans ce cas un périphérique d'enregistrement est trouvé et les débuts d'enregistrement automatiquement :

« Hôte du 20 juin 21:16:19 user.info acanosrv02 : serveur : **INFORMATION** : périphérique d'enregistrement 1 : disponible (enregistrements 1) »

Si l'enregistrement échoue alors contrôle si un périphérique d'enregistrement est trouvé :

« Hôte du 20 juin 21:16:19 user.info acanosrv02 : serveur : **INFORMATION** : Aucun périphérique d'enregistrement trouvé ».

Si vous voyez un tel avertissement, vérifiez le certificat en confiance d'enregistreur pour s'assurer qu'elle est la correcte utilisée par les CB.

Vérifiez le Syslog pour voir si la mémoire NFS est montée :

Si la mémoire NFS n'est pas montée, vous verrez « pour monter la mémoire NFS ».

Vérifiez que le répertoire et positionnement NFS sur le serveur d'enregistreur : /Folder-name est identique comme ce qui est configuré sur la mémoire NFS.

Exécutez l'API pour vérifier les alarmes qui associent à l'enregistreur :

https://<callBridge_IP>api/v1/system/alarms

S'il y a bas espace disque vous devriez voir le « recorderLowDiskSpace ».

Vérifiez alors que la mémoire NFS référencée par l'enregistreur a assez d'espace disque.