Configurar o gravador na ponte de chamada CMS/Acano

Contents

Introduction

Este documento descreve as etapas de configuração necessárias para configurar o Gravador no componente Call Bridge (CB) de um Cisco Meeting Server (CMS).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CMS 1.9 ou posterior
- Postman do Google Chrome
- Application Program Interface (API) do 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O CMS Recorder está disponível na versão 1.9 do servidor CMS (antigo Acano). O Gravador fornece a capacidade de gravar reuniões e salvar as gravações em um armazenamento de documentos NFS (Network File System).

O Gravador comporta-se como um cliente Extensible Messaging and Presence Protocol (XMPP), de modo que o servidor XMPP deve ser ativado no servidor que hospeda a Call Bridge.

A licença do gravador é necessária e deve ser aplicada no componente CallBridge, e não no servidor do Gravador.

O diretório Network File System (NFS) é necessário e pode ser configurado no Windows Server ou Linux.

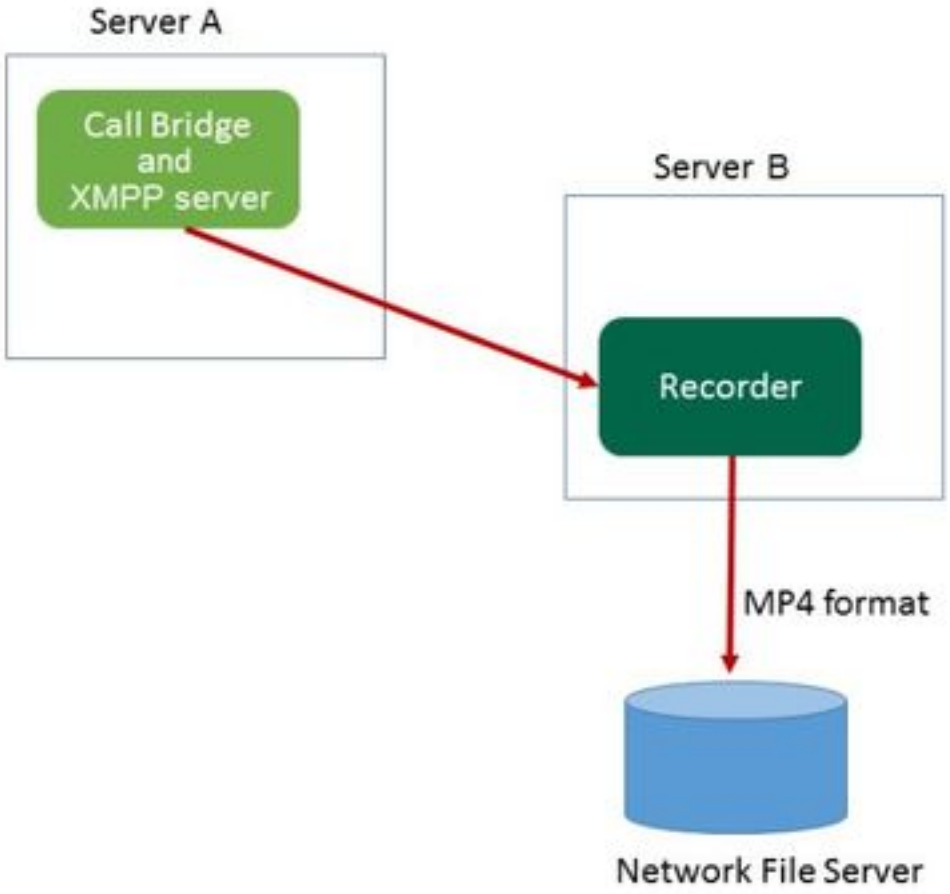
- Para o servidor Windows, siga as etapas para Implantar o sistema de arquivos de rede no Windows
- Para Linux, siga as etapas para implantar o sistema de arquivos de rede no Linux

  Note: Para NFS executado no Windows Server 2008 R2, há uma correção para problema de permissão.

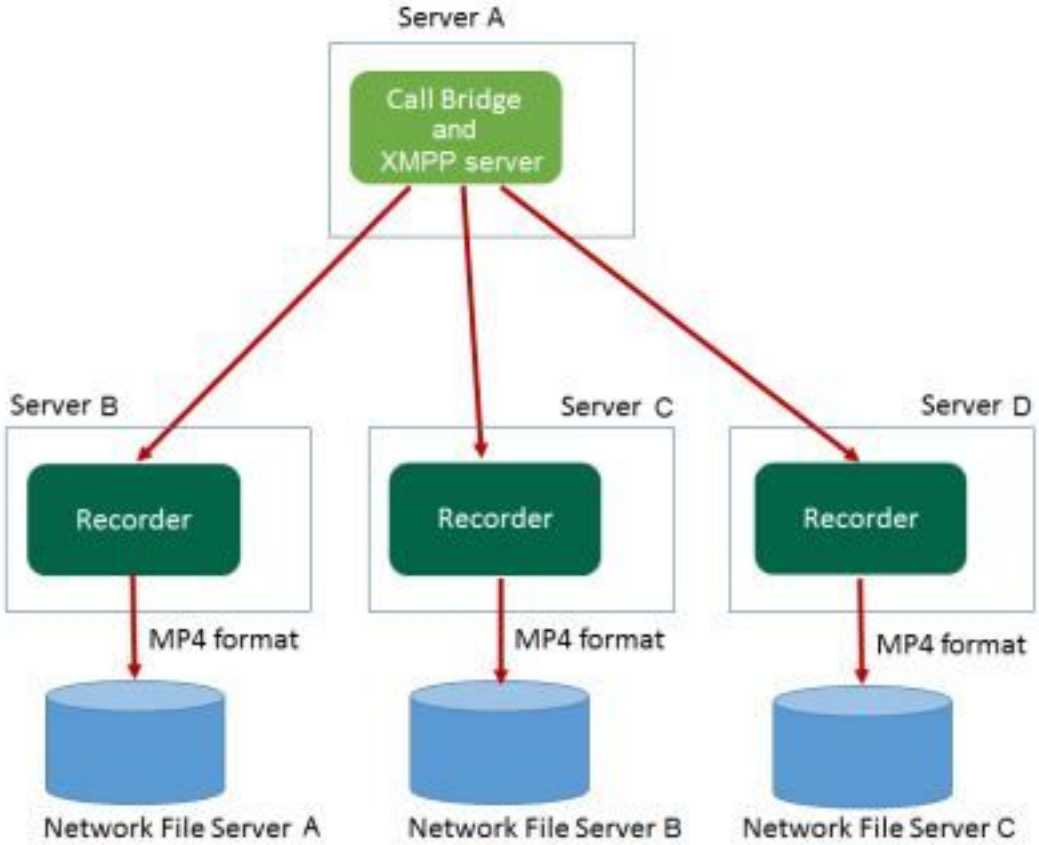
Implantações

Implantações suportadas

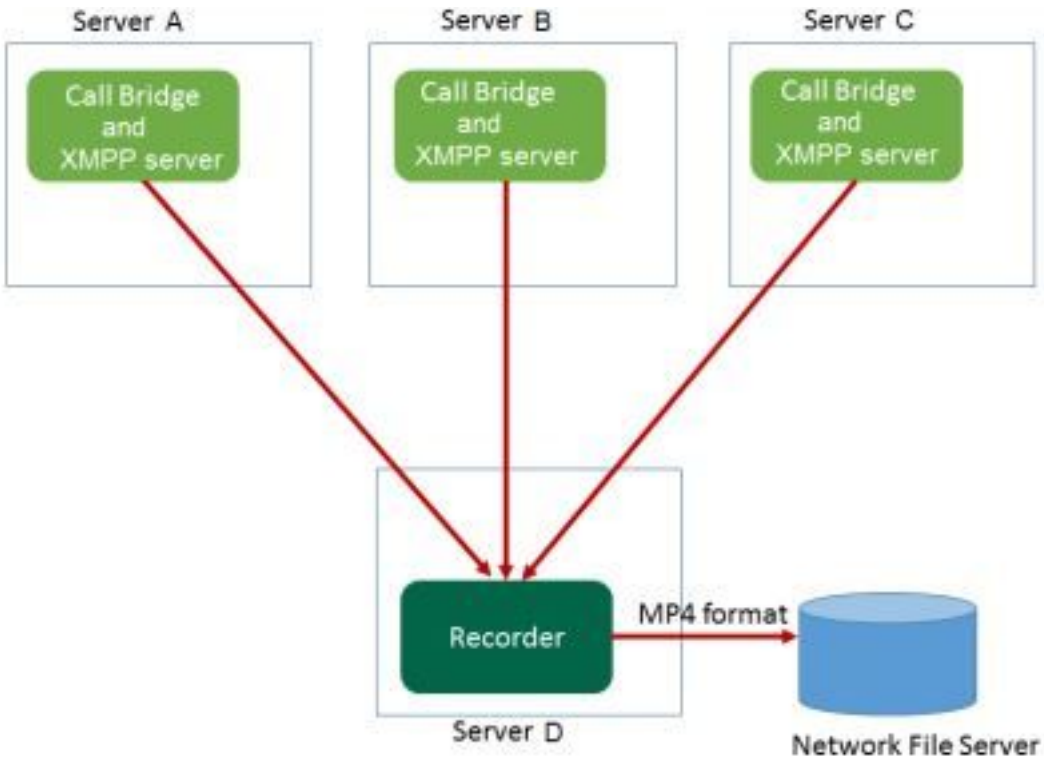
1. O Gravador deve ser hospedado em um servidor CMS/Acano remoto para o servidor que hospeda o CB, como mostrado nesta imagem



2. Também há suporte para a implantação redundante do Gravador. Se a redundância for configurada, as gravações serão balanceadas entre todos os dispositivos de gravação (servidores). Isso significa que cada CB usa cada Gravador disponível, conforme mostrado nesta imagem

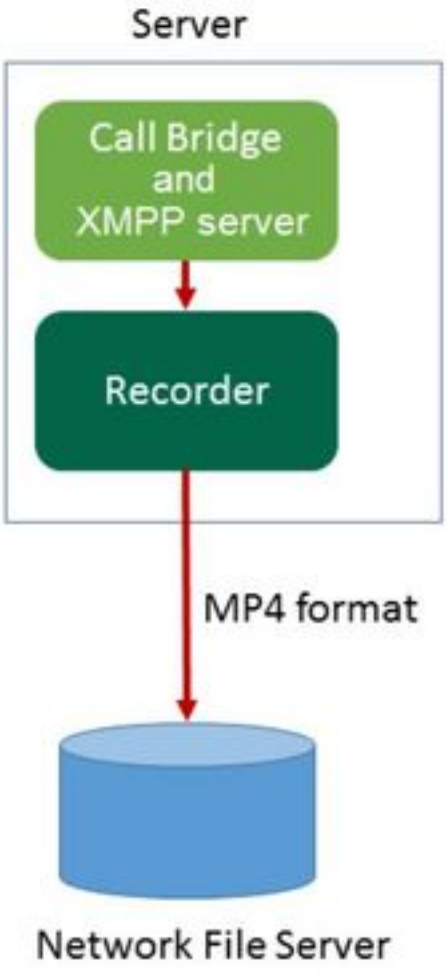


3. O mesmo se aplica no caso contrário, quando existem múltiplos BC. Todos os nós CB usam o Gravador disponível para eles, como mostrado nesta imagem



Outra configuração

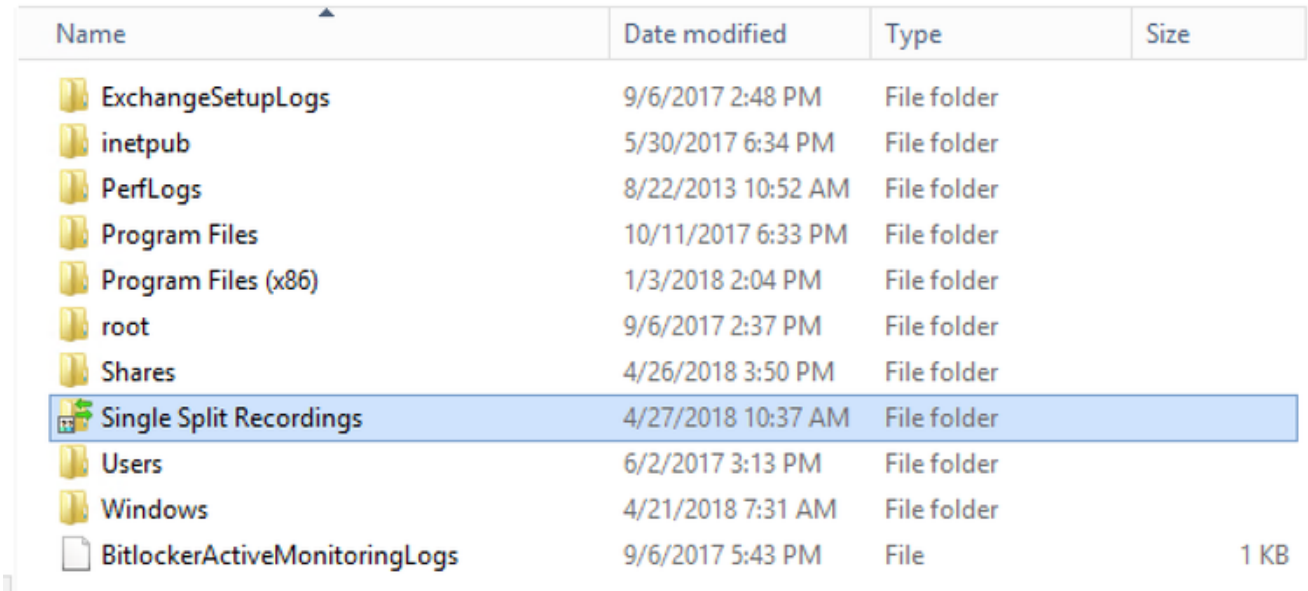
O Gravador também pode ser hospedado no mesmo servidor que o CB, mas isso deve ser usado apenas para testes ou implantações muito pequenas, veja a próxima imagem para referência. A desvantagem aqui é que somente 1 a 2 gravações simultâneas são possíveis:



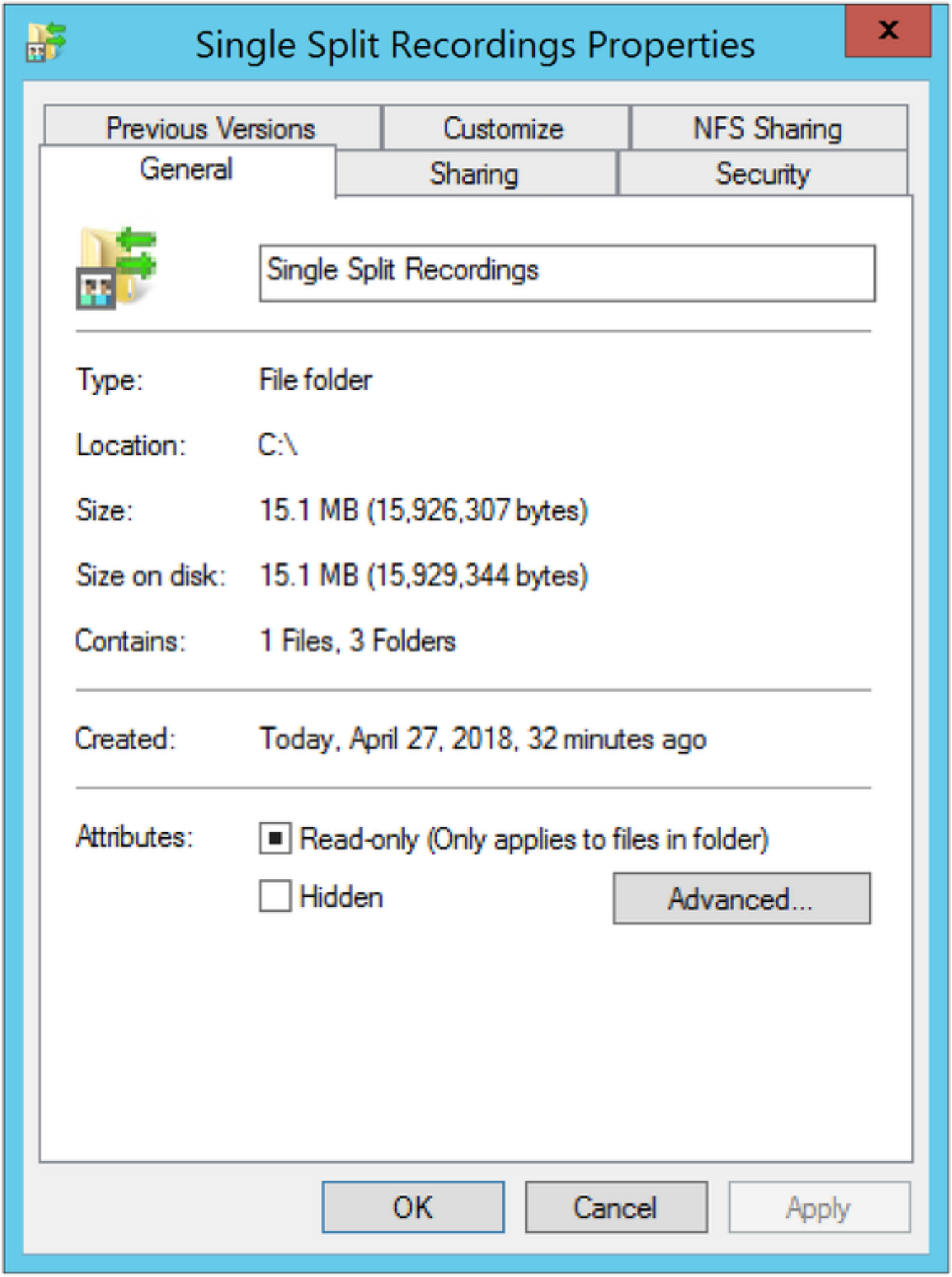
Configurar

Etapa 1. Configurar uma Pasta de Compartilhamento NFS em um Windows Server

a. Usando o Windows Explorer, crie uma nova pasta para seu compartilhamento NFS. Neste exemplo, uma pasta chamada **Gravações de Divisão Única** foi criada no meu disco local



b. Clique com o botão direito do mouse na pasta e selecione **Propriedades**



c. Selecione a guia **Compartilhamento NFS** na parte superior direita. Mostra a pasta como **Não compartilhada**. Neste exemplo, a pasta foi compartilhada anteriormente, caso contrário, você deverá ver um caminho de rede em branco e a pasta será exibida como **Não compartilhada**

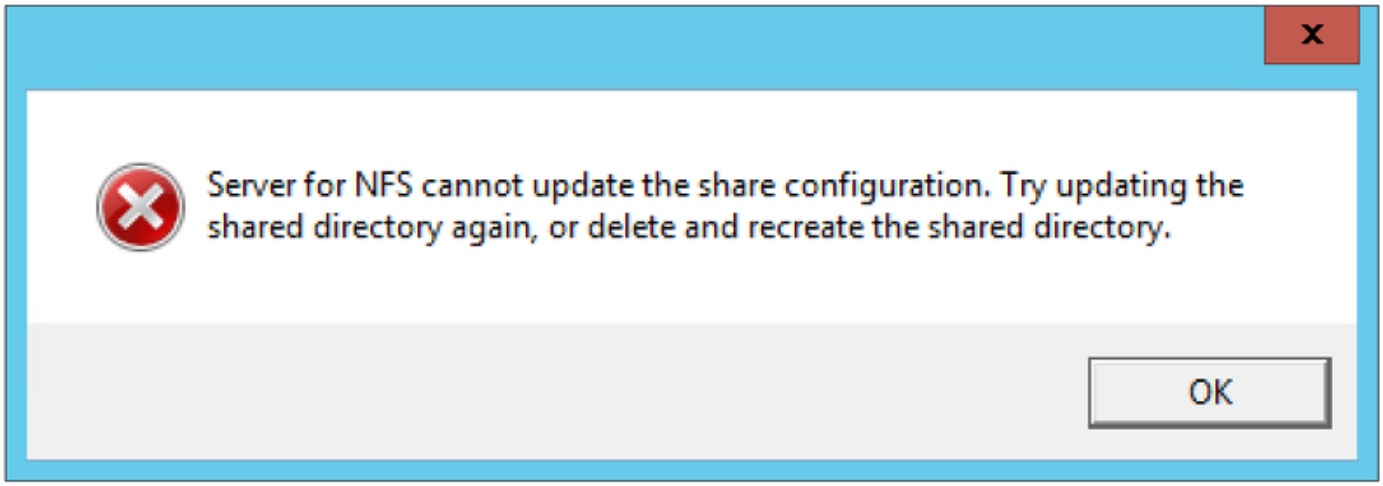
d. Selecionar **Gerenciar Compartilhamento NFS**

e. Marcar a caixa de seleção ao lado de **Compartilhar esta pasta**

f. Digite o nome do compartilhamento de pasta no **nome de compartilhamento** sem espaço

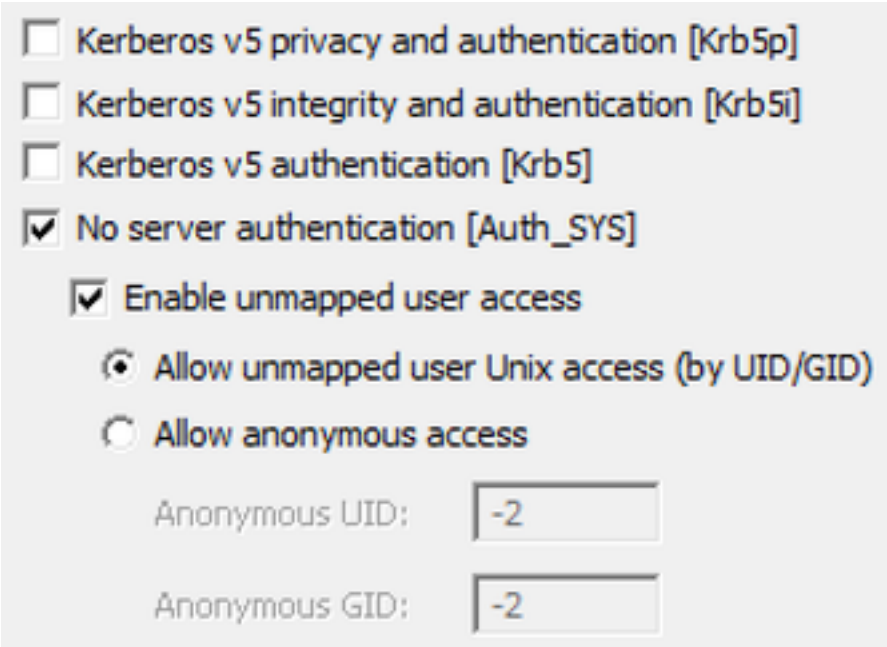
> **Note**: Isso é usado pelos clientes NFS e pelo gravador CMS para localizar essa pasta.

> **Note**: Certifique-se de que não há espaço(s) no nome do compartilhamento de pasta. Se houver, você não poderá salvar suas alterações e esta janela de erro será exibida:



g. Deixe a codificação como padrão **ANSI** valor

h. Por padrão, todas as caixas de seleção de autenticação estão marcadas. Desmarque todos os **Kerberos** opções de autenticação que deixam somente os **Sem autenticação de servidor [Auth_SYS]**



I. Selecionar **Permitir acesso Unix de usuário não mapeado (por UID/GID)**

j. Na parte inferior, selecione **Permissões** para definir permissões no compartilhamento de rede

> **Note**: O padrão é Read-Only (Somente leitura) para todas as máquinas. O gravador deve ter

acesso de leitura e gravação, para que você possa alterar o padrão para **TODAS AS MÁQUINAS** ou adicionar regras específicas para o gravador. A melhor prática seria desativar o acesso a TODAS AS MÁQUINAS alterando-o para **Sem Acesso** e adicionando nova permissão para o IP dos servidores que precisam de acesso ao compartilhamento.

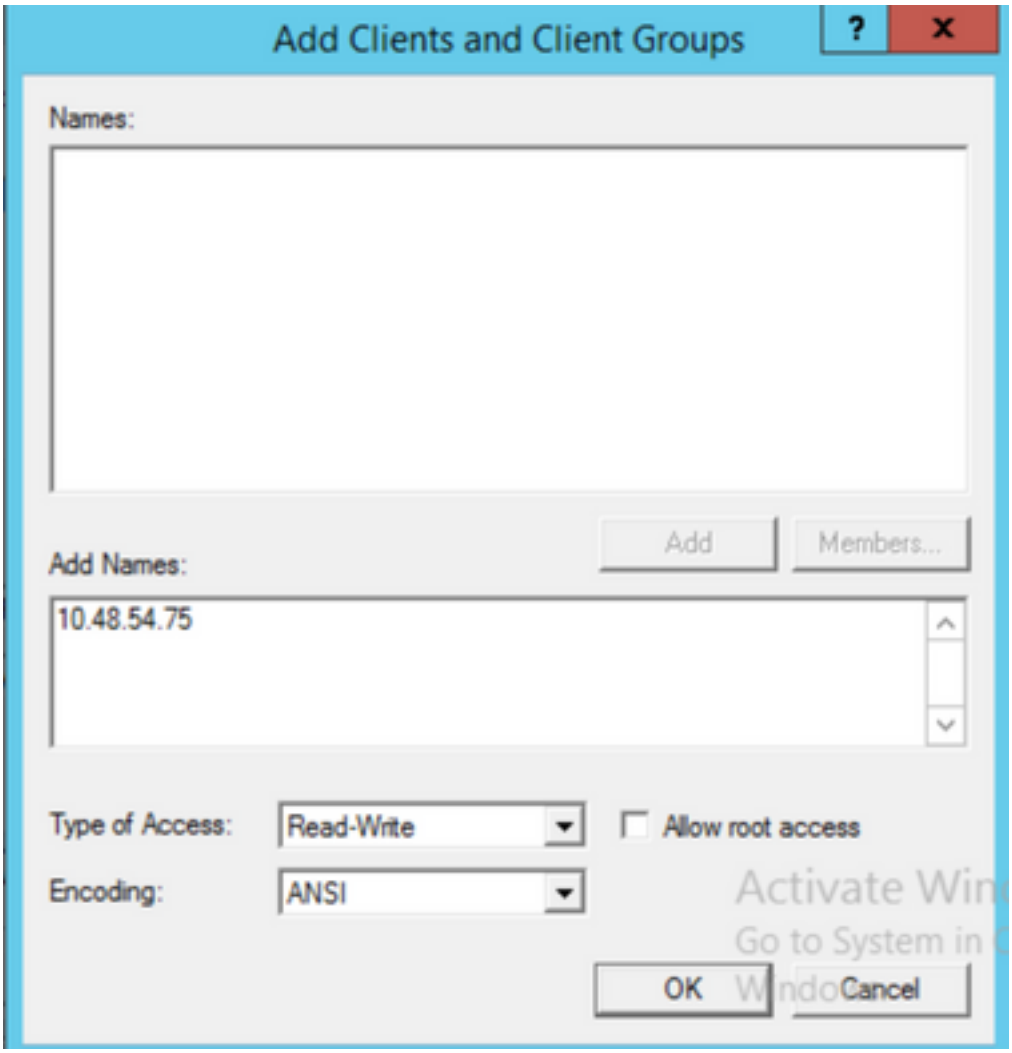
k. Para adicionar permissão ao gravador, selecione **adi**

I. IN **Adicionar nomes**, insira o endereço IP do servidor do Gravador. Neste exemplo, meu servidor de gravador é 10.48.54.75

m. Selecionar **Leitura-gravação** acesso

n. Deixe a codificação como **ANSI**

o. Sair **Permitir acesso raiz** Desabilitado



p. Selecione **OK** para fechar a caixa de diálogo de permissões

p. Selecionar **TODAS AS MÁQUINAS**

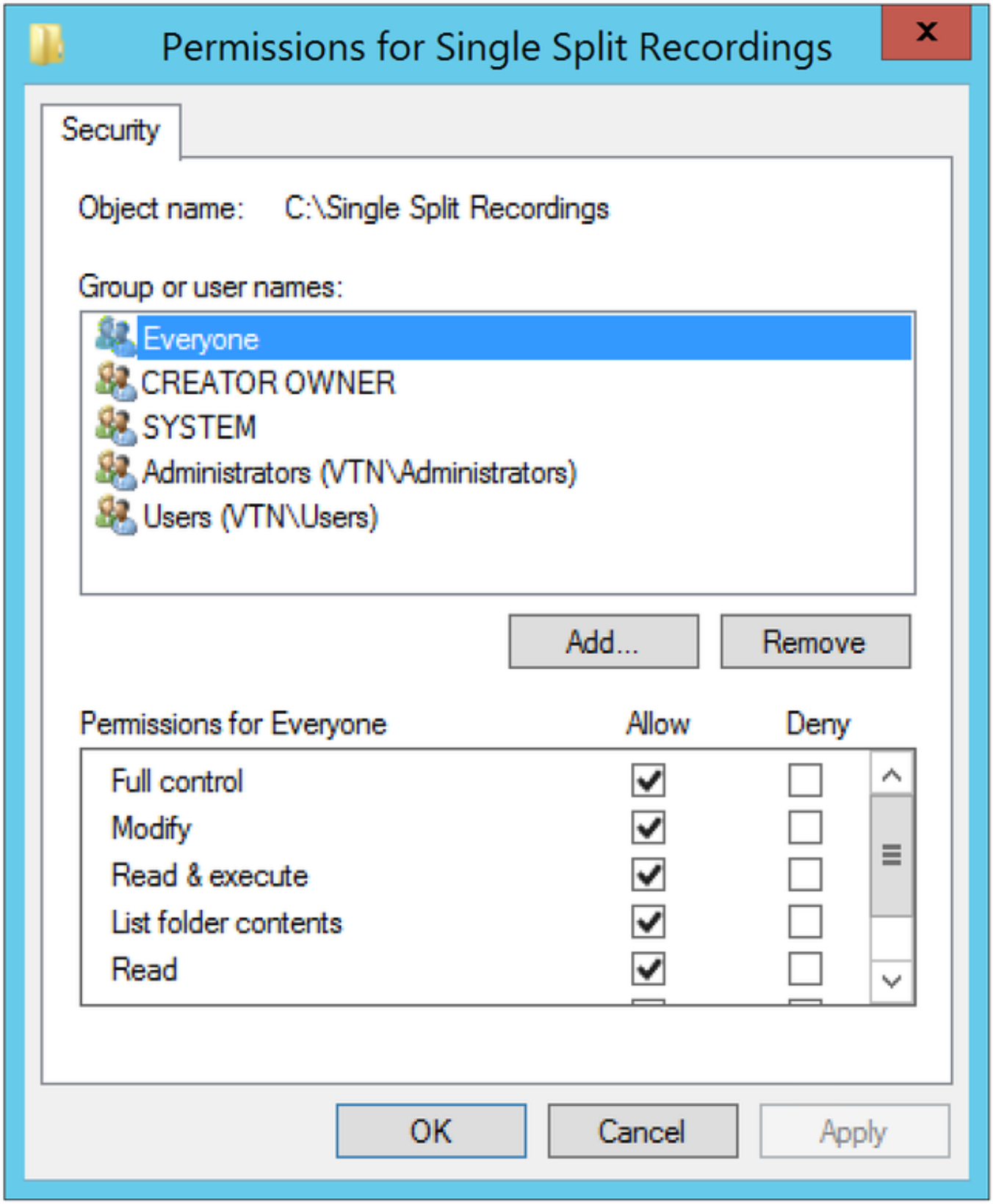
r. alteram **Tipo de acesso** para **Sem acesso**

s. Selecionar **OK** para fechar a janela de permissões

t. Selecionar **OK** novamente para retornar à janela Propriedades da pasta

u. Selecionar **Security**

Note: O grupo **Todos** deve ter acesso total à pasta. Se não estiver listado, selecione **Editar** para abrir o editor de permissões. Selecione **Add** para adicionar um usuário e, no campo de nomes, digite **All (Todos)** e selecione OK. Selecione **Todos** na lista, marque a caixa de seleção **Controle total** e selecione **OK**. Selecione **OK** novamente para fechar as propriedades. Se configurado corretamente, ele se assemelha à próxima imagem:



Etapa 2. Configurar e ativar o gravador no servidor do Gravador

a. Configure o Gravador para ouvir na(s) interface(s) de sua escolha com este comando:

gravador ouve <interface[:port] whitelist>

b. Se o gravador estiver no BC local, a interface deverá ser definida como "loopback", portanto, use este comando:

escuta do gravador lo:8443

c. Se for para ouvir em uma interface específica, digamos "a", então use isto:

gravador ouvir a:8443

> **Note**: Se você configurar o gravador em um nó do CB clusterizado, a interface deverá ser a interface de escuta local do nó no qual o gravador está sendo configurado.

d. Defina o arquivo de certificado a ser usado pelo gravador. Você pode usar um certificado que já existe e um arquivo de chave privada usado pelo CB, por exemplo.

gravador certs <keyfile> <certificate file>

e. Adicione o certificado CB ao repositório confiável do Gravador usando o comando:

register trust <crt-bundle>

O pacote crt deve conter o certificado utilizado pelo BC, se diferente. Se estiver em um cluster, deverá conter os certificados de cada CB no cluster.

f. Especifique o nome do host ou o endereço IP do NFS e o diretório no NFS para Armazenar as gravações:

gravador nfs <hostname/IP>:<diretory>

> **Note**: O Gravador não autentica para o NFS, mas é importante que o Recorder Server tenha acesso de leitura/gravação ao diretório NFS.

g. Ative o Gravador com o uso do comando:

gravador habilitado

Etapa 3. Criar um usuário de API no CB

Crie um usuário de API no CB, o que é necessário para outras configurações usando a função API:

Crie o usuário com estas etapas:

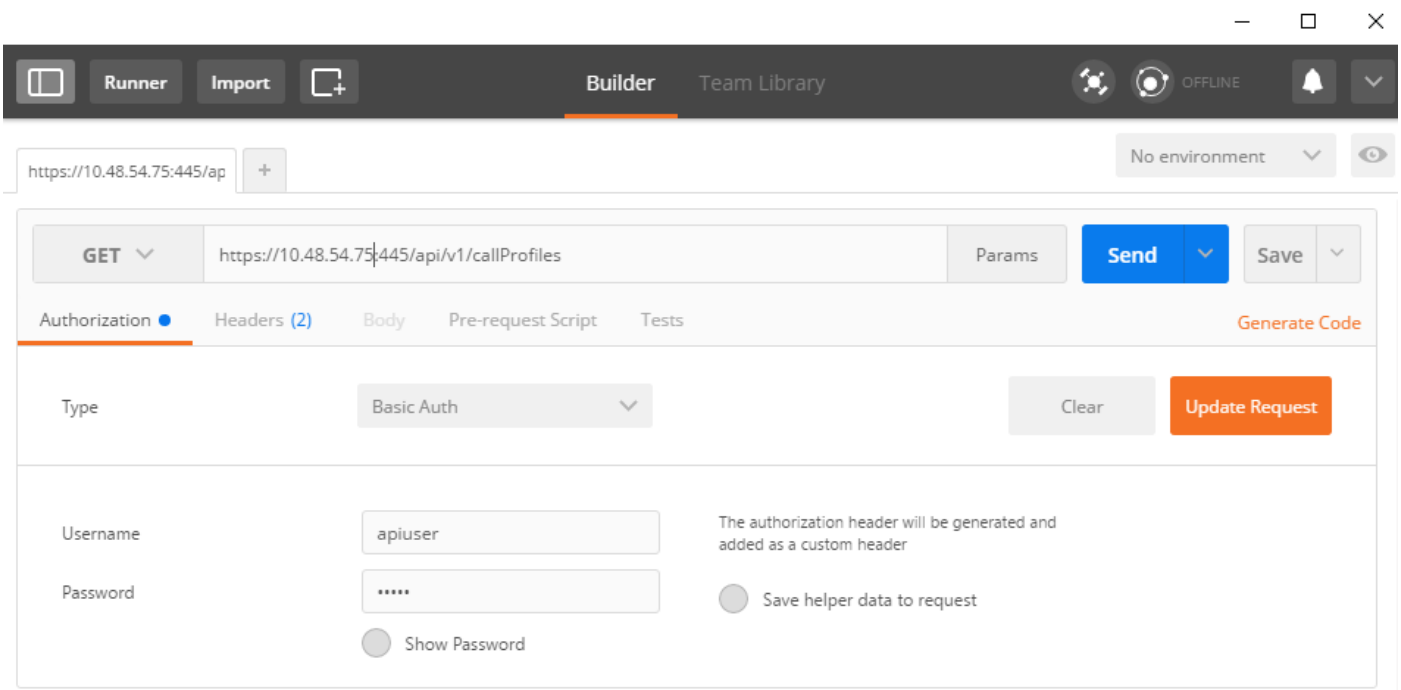
a. Conecte-se via Secure Shell (SSH) ou console ao CB com o uso das credenciais de administrador.

b. O usuário adiciona **<username>** api e, em seguida, pressione a tecla **Return** e digite a senha seguida pela tecla **Return**.

Etapa 4. Adicione o Gravador ao CB usando a API

1. Baixe e instale o Postman aqui

2. Insira a URL de acesso da API na barra de endereço, por exemplo: **https://<Callbridge_IP>:445/api/v1/<entity>**. Em seguida, defina na autenticação o nome de usuário e a senha da Etapa 3, em Autorização com **Autenticação básica** como tipo



> **Note**: Pressupõe-se que não há atualmente nenhum gravador ou callProfile configurado no CB. Caso contrário, você pode modificar um gravador existente e/ou callProfile com o uso do método PUT.

3. Adicione o gravador ao CB com a API

a. Envie um POST vazio com https://<Callbridge_IP>:445/api/v1/gravadores

b. Enviar um GET com a mesma URL na (a), copiar a ID do gravador, sem os orçamentos para o Bloco de Notas

c. Defina o URL do gravador enviando um PUT com

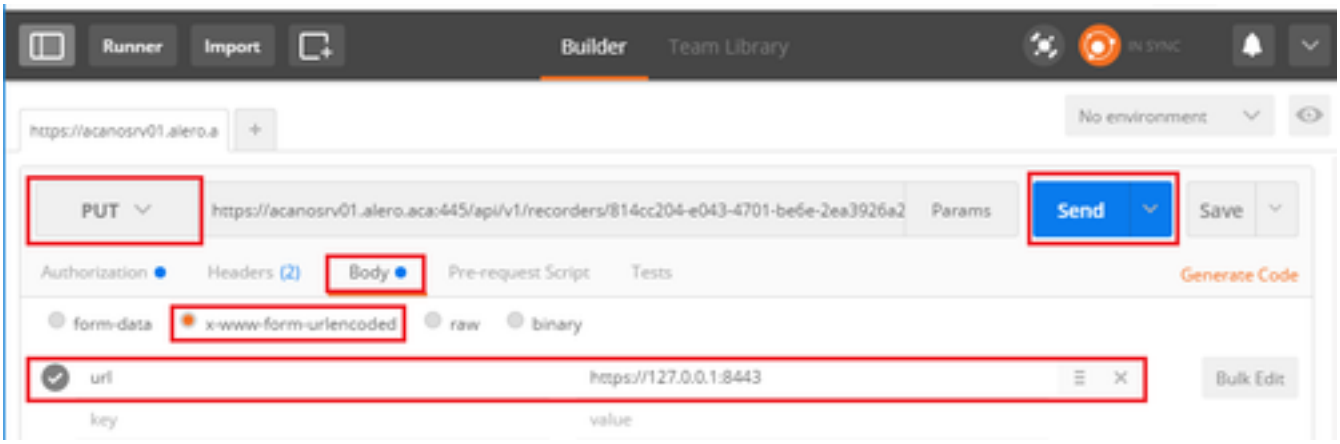
https://<Callbridge_IP>:445/api/v1/recorders/<gravid> e adicione-o no BODY antes de executar o PUT:

url=https://127.0.0.1:8443 (se o gravador estiver no BC local)

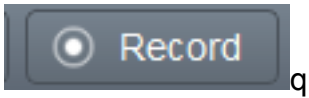
or

url=https://<IP Address of recorder>:8443 (se o gravador não estiver no CB local)

Por exemplo:



Note: **dtmfProfile**, **callProfile** e **callLegProfile** são particularmente importantes para os endpoints SIP que participam de uma conferência de espaço em grupo. Eles permitem que o endpoint possa iniciar/parar a gravação de uma chamada para/do espaço.

A partir do CMA 1.9.3 e do CMS 2.0.1, os tons de DTMF não são necessários agora que há o comando 

que é adicionado ao cliente quando o gravador está presente ou é conhecido pelo callbridge ao qual o cliente está conectado. O botão de registro também foi adicionado ao WebRTC do CMS 2.3.

4. Criar um callProfile

a. Envie um POST vazio com **https://<Callbridge_IP>:445/api/v1/callProfiles**

b. Enviar um GET com a mesma URL na (a), copiar a ID callProfile, sem os orçamentos para o Bloco de Notas

c. Defina o modo de gravação no callProfile enviando um PUT com **https://<Callbridge_IP>:445/api/v1/callProfiles/<call profile ID>** e adicione o no BODY antes de executar o PUT.

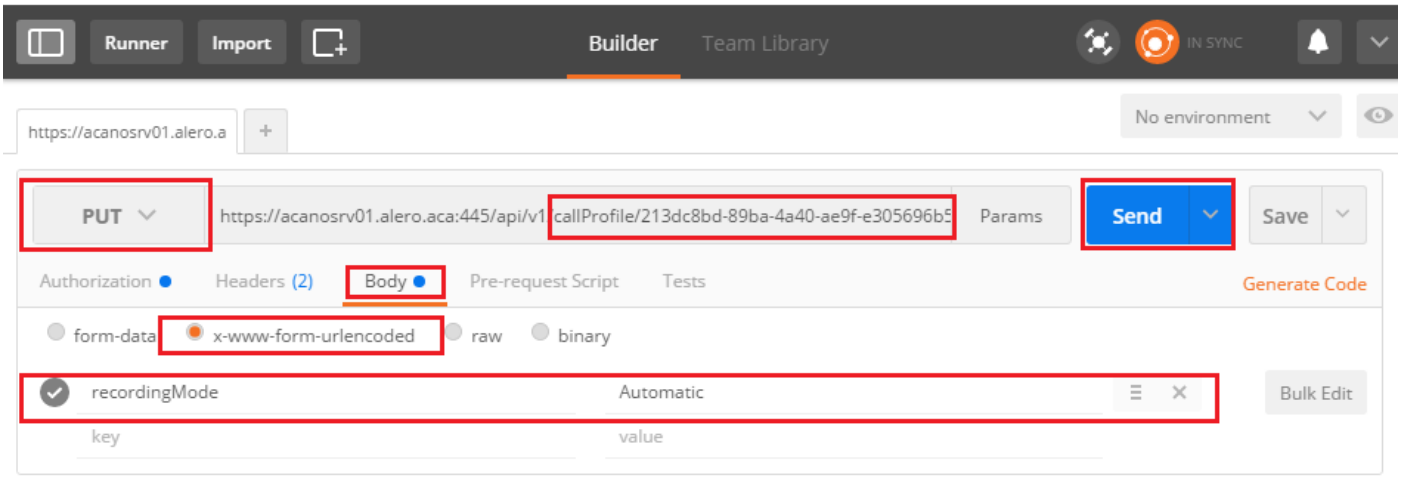
recordingMode=Manual (se quiser que os chamadores comecem a gravar usando entradas DTMF)

or

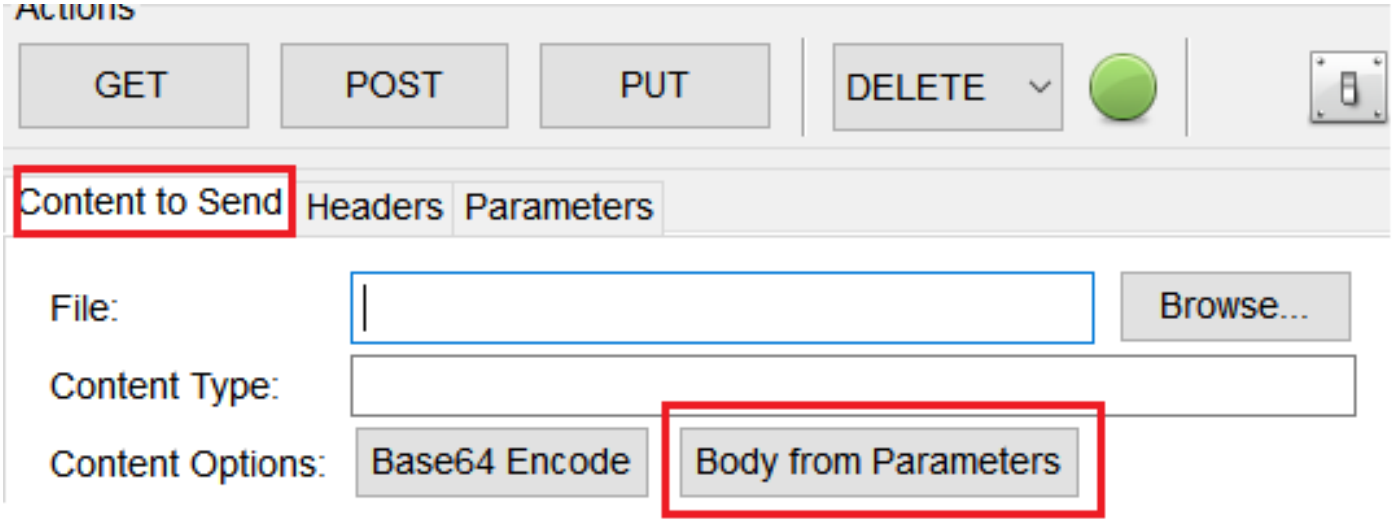
recordingMode=Automático (se a gravação for iniciada automaticamente quando as chamadas

forem iniciadas)

Por exemplo:



Note: Se você usa o POSTER do firefox, é necessário selecionar **Conteúdo a Enviar** e selecionar **Corpo dos Parâmetros** antes de enviar o PUT/POST, dessa forma, ele é compilado nos códigos que o BC pode entender. Como na próxima imagem:



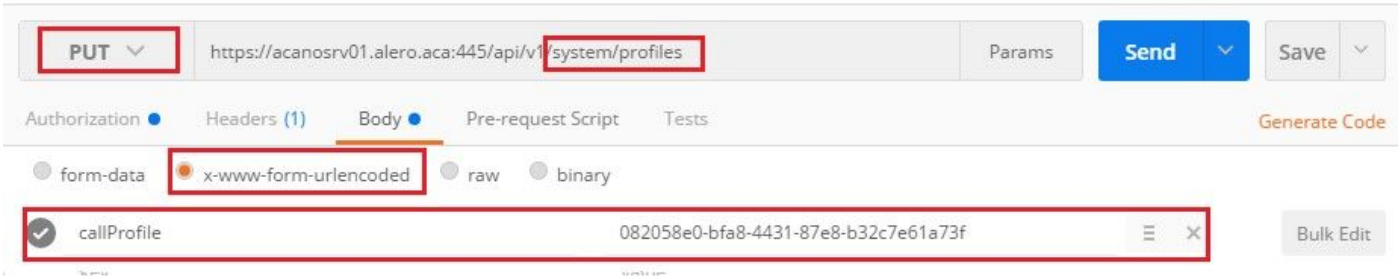
5. Adicionar perfil de chamada aos perfis do sistema

O callProfile define se as chamadas podem ser gravações e se podem ser feitas com ou sem intervenção do usuário.

Envie um PUT com https://<Callbridge_IP>:445/api/v1/system/profiles depois de adicionar callProfile no BODY

callProfile=<call profile ID>

Por exemplo:

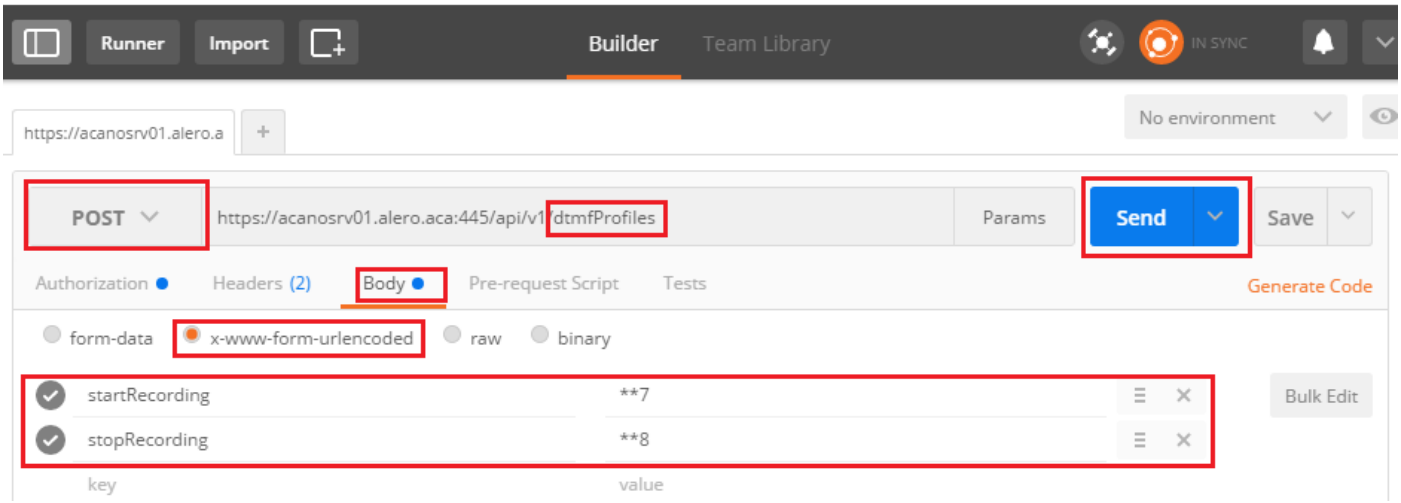


Se o modo de gravação estiver definido como Manual, você deverá definir um perfil DTMF para definir como os usuários podem iniciar e parar gravações usando tons DTMF.

6. Criar o perfil DTMF

a. Envie uma postagem com https:// <Callbridge_IP>:445/api/v1/dtmfProfiles depois de definir startRecording=**7 e stopRecording=**8 (por exemplo) no BODY como startRecording=**7&stopRecording=**8.

Por exemplo:



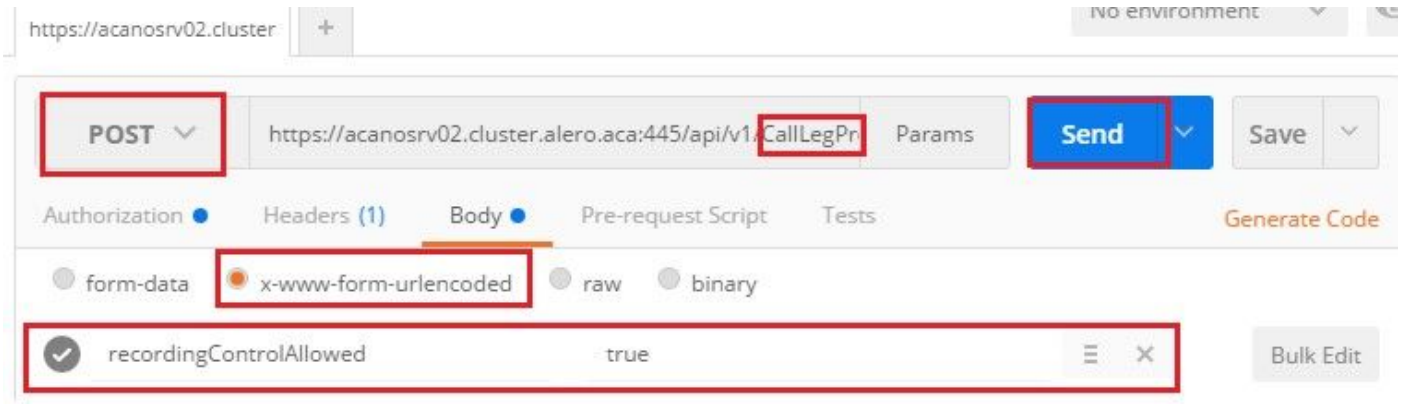
b. Envie um GET para ver o novo perfil DTMF e copie a ID sem os orçamentos para o bloco de notas.

7. Criar perfil CallLeg

CallLegProfiles determina o comportamento na chamada. Nesse caso, ele determina se uma chamada pode ser gravada.
Crie um perfil de leg da chamada da seguinte maneira:

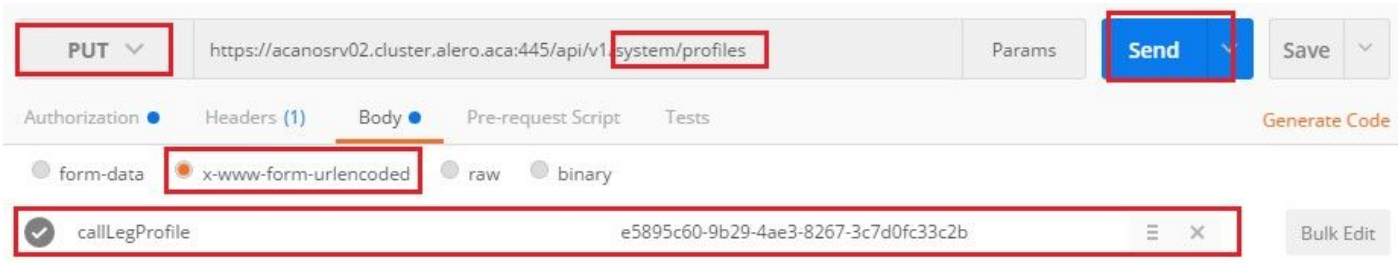
a. Envie uma postagem com https://<Callbridge_IP>:445/api/v1/CallLegProfiles depois de adicionar recordControlAllowed=true no BODY:

Por exemplo:



b. Aplique o CallLegProfile, enviando um PUT com https://<Callbridge_IP>:445/api/v1/system/files e adicionando callLegProfile=<callLegProfile_ID> no BODY:

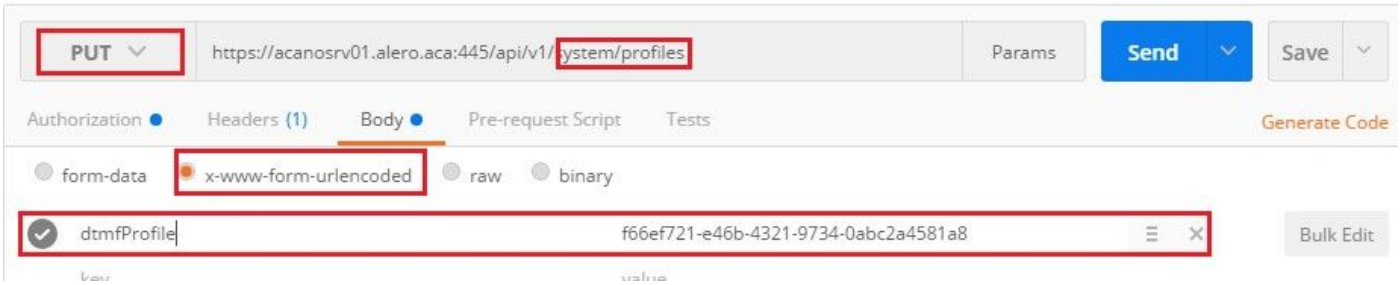
Por exemplo:



8. Aplicar o perfil DTMF:

Envie um PUT com https://<Callbridge_IP>:445/api/v1/system/files depois de adicionar o dtmfProfile em BODY dtmfProfile=<dfmt Profile ID>

Por exemplo:



Verificar

Esta seção fornece informações para confirmar se a sua configuração funciona corretamente.

1. Depois de configurado, verifique seu status com esses comandos, você poderá obter uma saída semelhante à da próxima imagem

gravador

CB autônomo local:

```
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 se CB agrupado:

```
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. Enviar um GET para visualizar o perfil do sistema, você deve ver a **callProfile**, **CallLegProfile** e **dtmfProfile** (supondo que todos eles tenham sido configurados) no resultado com

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

Por exemplo:

```
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. Para verificar o que foi configurado no CallProfile, use-o na API

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

Mostra que os métodos de gravação foram definidos, seja Automático ou Manual, conforme mostrado:

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

4. Para verificar o que está configurado no CallLegProfile, use esta API

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

Saída de exemplo:

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

5. Para verificar o que foi configurado no perfil DTMF, use-o na API

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

Isso mostra que os métodos de gravação foram definidos, seja Automático ou Manual, conforme mostrado:

```
<?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: Os perfis DTMF não funcionam em chamadas ponto a ponto, portanto, você só pode usar a gravação manual em um espaço.

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Para exibir o que está sendo registrado em relação ao gravador, execute o comando:

syslog siga

A saída exibida é semelhante a esta:

```
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
```

Neste exemplo, acanosrv05 é o servidor que hospeda o gravador e os outros nós CB conectados a ele são 10.48.54.75 e 10.48.54.76.

Isso mostra que o CB remoto está se conectando e autenticando corretamente com o Gravador.

Se o gravador for local para o BC, a conexão virá do IP de 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
```

> **Note**: A maioria dos registros relacionados aos processos do gravador são mostrados no syslog como proxy do gravador, que fornecem uma indicação de onde o gravador pode estar falhando.

Outros syslogs são mostrados da seguinte forma para o gravador:

Nesse caso, um dispositivo de gravação é encontrado e a gravação é iniciada automaticamente:

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

Se a gravação falhar, verifique se um dispositivo de gravação foi encontrado:

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

Se vir esse aviso, verifique o certificado na confiança do gravador para garantir que ele seja o correto usado para configurar o CB.

Verifique o syslog para ver se o armazenamento NFS está montado:

- Se o armazenamento NFS não estiver montado, "Falha ao montar o armazenamento NFS" será exibido
- Verifique e certifique-se de que a pasta NFS definida no servidor do gravador:/Nome da pasta é igual ao que está configurado no armazenamento NFS

Execute a API para verificar os alarmes relacionados ao gravador:

- **https://<callBridge_IP>api/v1/sistema/alarmes**
- Se houver pouco espaço em disco, a mensagem "gravadorBaixoEspaçoEmDisco" será exibida
- Em seguida, verifique se o armazenamento NFS referenciado pelo gravador tem espaço em disco suficiente

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems