Fixe o tronco do SORVO entre o exemplo de configuração CUCM e de VCS

Índice

Introdução

Este documento descreve como estabelecer uma conexão segura do Session Initiation Protocol (SIP) entre o gerente das comunicações unificadas de Cisco (CUCM) e o server de comunicação de vídeo do Cisco TelePresence (VCS).

Os CUCM e o VCS são integrados proximamente. Porque os pontos finais de vídeo podem ser registrados no CUCM ou no VCS, os troncos do SORVO devem existir entre os dispositivos.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Gerente das comunicações unificadas de Cisco
- Server de comunicação de vídeo do Cisco TelePresence
- Certificados

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas. Este exemplo usa a versão de software X7.2.2 do VCS de Cisco e a versão 9.x CUCM.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Assegure-se de que os Certificados sejam válido, adicionar os Certificados aos server CUCM e de VCS de modo que confiem Certificados de cada um, a seguir estabelecem o tronco do SORVO.

Diagrama de Rede

Obtenha o certificado do VCS

Àrevelia, todos os sistemas do VCS vêm com certificado provisório. Na página de admin, navegue ao > gerenciamento de certificado > ao **certificado de servidor da manutenção**. Clique o **certificado do show server**, e uma nova janela abre com os dados brutos do certificado:

Este é um exemplo dos dados crus do certificado:

```
-----BEGIN CERTIFICATE-----
MIIDHzCCAoigAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmjFDMEEGA1UECgw6VGVt
cG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTFlMy1hNTE4LTAwNTA1
Njk5NWI0YjFDMEEGA1UECww6VGVtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYw
LTI5YTAtMTFlMy1hNTE4LTAwNTA1Njk5NWI0YjEOMAwGA1UEAwwFY2lzY28wHhcN
MTMwOTMwMDcxNzIwWhcNMTQwOTMwMDcxNzIwWjCBmjFDMEEGA1UECgw6VGVtcG9y
YXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTFlMy1hNTE4LTAwNTA1Njk5
NWI0YjFDMEEGA1UECww6VGVtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5
YTAtMTFlMy1hNTE4LTAwNTA1Njk5NWI0YjEOMAwGA1UEAwwFY2lzY28wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKWvob+Y1zrKoAB5BvPsGR7aVfmTYPipL0I/
L21fyyjoO5qv9lzDCgy7PFZPxkD1d/DNLIgp1jjUqdfFV+64r8OkESwBO+4DFlut
tWZLQ1uKzzdsmvZ/b41mEtosElHNxH7rDYQsqdRA4ngNDJVlOgVFCEV4c7ZvAV4S
E8m9YNY9AgMBAAGjczBxMAkGA1UdEwQCMAAwJAYJYIZIAYb4QgENBBcWFVRlbXBv
cmFyeSBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU+knGYkeeiWqAjORhzQqRCHba+nEw
HwYDVR0jBBgwFoAUpHCEOXsBH1AzZN153S/Lv6cxNDIwDQYJKoZIhvcNAQEFBQAD
gYEAZklIMSfi49p1jIYqYdOAIjOiashYVfqGUUMFr4V1hokM90ByGGTbx8jx6Y/S
p1SyT4ilU5uiY0DD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7
1Zc3zTl6WL6hsj+90GAsI/TGthQ2n7yUWPl6CevopbJe1iA=
-----END CERTIFICATE-----
```

Você pode descodificar o certificado e ver os dados do certificado com o uso do OpenSSL em seu PC local ou o uso de um decodificador em linha do certificado tal como o cliente SSL:

Gerencia e transfira arquivos pela rede o certificado auto-assinado do VCS

Porque cada server do VCS tem um certificado com o mesmo Common Name, você precisa de pôr Certificados novos sobre o server. Você pode escolher usar os certificados auto-assinados ou os Certificados assinados pelo Certificate Authority (CA). Veja a criação e o uso do certificado do Cisco TelePresence com o guia de distribuição do VCS de Cisco para detalhes deste procedimento.

Este procedimento descreve como usar o VCS próprio para gerar um certificado auto-assinado, a seguir transfere arquivos pela rede esse certificado:

1. Entre como a raiz ao VCS, comece o OpenSSL, e gerencia uma chave privada:

```
~ # openssl
OpenSSL> genrsa -out privatekey.pem 1024
Generating RSA private key, 1024 bit long modulus
.................................++++++
.............++++++
e is 65537 (0x10001)
```

2. Use esta chave privada a fim gerar uma solicitação de assinatura de certificado (CSR):

```
OpenSSL> req -new -key privatekey.pem -out certcsr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BE
State or Province Name (full name) [Some-State]:Vlaams-Brabant
Locality Name (eg, city) []:Diegem
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:radius.anatomy.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
OpenSSL> exit
```

3. Gerencia o certificado auto-assinado:

```
~ # openssl x509 -req -days 360 -in certcsr.pem -signkey privatekey.pem -out vcscert.pem
Signature ok
subject=/C=BE/ST=Vlaams-Brabant/L=Diegem/O=Cisco/OU=TAC/CN=radius.anatomy.com
Getting Private key
~ #
```

4. Confirme que os Certificados estão agora disponíveis:

```
~ # ls -ltr *.pem
-rw-r--r-- 1 root root 891 Nov 1 09:23 privatekey.pem
-rw-r--r-- 1 root root 664 Nov 1 09:26 certcsr.pem
-rw-r--r-- 1 root root 879 Nov 1 09:40 vcscert.pem
```

5. Transfira os Certificados com WinSCP, e transfira-os arquivos pela rede no Web page assim

que o VCS pode usar os Certificados; você precisa a chave privada e o certificado gerado:

6. Repita este procedimento para todos os server do VCS.

Adicionar o certificado auto-assinado do server CUCM ao server do VCS

Adicionar os Certificados dos server CUCM de modo que o VCS os confie. Neste exemplo, você está usando os certificados auto-assinados padrão de CUCM; CUCM gerencie certificados auto-assinados durante a instalação assim que você não precisa de criar aqueles como você fez no VCS.

Este procedimento descreve como adicionar um certificado auto-assinado do server CUCM ao server do VCS:

1. Transfira o certificado CallManager.pem do CUCM. Registre no OS a página de administração, navegue à Segurança **> ao** CertificateManagement**, a seguir** selecione e transfira o certificado auto-assinado CallManager.pem:

2. Adicionar este certificado como um certificado de CA confiado no VCS.On o VCS, navegue ao **>** gerenciamento de certificado da **manutenção > certificado de CA confiado**, e selecione o **certificado de CA da mostra**:

   Uma nova janela abre com todos os Certificados que são confiados atualmente.

3. Copie todos os atualmente certificados confiáveis a um arquivo de texto. Abra o arquivo CallManager.pem em um editor de texto, copie seu índice, e adicionar esse índice à parte inferior do mesmo arquivo de texto após atualmente os certificados confiáveis:

```
CallManagerPub
======================
-----BEGIN CERTIFICATE-----
MIICmDCCAgGgAwIBAgIQZo7WOmjKYy9JP228PpPvgTANBgkqhkiG9w0BAQUFADBe
MQswCQYDVQQGEwJCRTEOMAwGA1UEChMFQ2lzY28xDDAKBgNVBAsTA1RBQzERMA8G
A1UEAxMITUZDbDFQdWIxDzANBgNVBAgTBkRpZWdlbTENMAsGA1UEBxMEUGVnMzAe
Fw0xMjA4MDExMDI4MzVaFw0xNzA3MzExMDI4MzRaMF4xCzAJBgNVBAYTAkJFMQ4w
DAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMREwDwYDVQQDEwhNRkNsMVB1YjEP
MA0GA1UECBMGRGllZ2VtMQ0wCwYDVQQHEwRQZWczMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDmCOYMvRqZhAl+nFdHk0Y2PlNdACglvnRFwAq/rNgGrPCiwTgc
0cxqsGtGQLSN1UyIPDAE5NufROQPJ7whR95KGmYbGdwHfKeuig+MT2CGltfPe6ly
c/ZEDqHYvGlzJT5srWUfM9GdkTZfHI1iV6k/jvPtGigXDSCIqEjn1+3IEQIDAQAB
o1cwVTALBgNVHQ8EBAMCArwwJwYDVR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMC
BggrBgEFBQcDBTAdBgNVHQ4EFgQUK4jYX6O6BAnLCalbKEn6YV7BpkQwDQYJKoZI
hvcNAQEFBQADgYEAkEGDdRdMOtX4ClhEatQE3ptT6L6RRAyP8oDd3dIGEOYWhA2H
Aqrw77loieva297AwgcKbPxnd5lZ/aBJxvmF8TIiOSkjy+dJW0asZWfei9STxVGn
NSr1CyAt8UJh0DSUjGHtnv7yWse5BB9mBDR/rmWxIRrlIRzAJDeygLIq+wc=
-----END CERTIFICATE-----
```

Se você tem os servidores múltiplos no CUCM aglomeram, adicionam todo aqui.

4. Salvar o arquivo como CATrust.pem, e clique o **certificado de** UploadCA **a fim** transferir arquivos pela rede o arquivo de volta ao VCS:

   O VCS confiará agora os Certificados oferecidos por CUCM.

5. Repita este procedimento para todos os server do VCS.

Transfira arquivos pela rede o certificado do server do VCS ao server CUCM

O CUCM precisa de confiar os Certificados oferecidos pelo VCS.

Este procedimento descreve como transferir arquivos pela rede o certificado que do VCS você gerou no CUCM como um certificado da CallManager-confiança:

1. Na página de administração do OS, navegue ao **>** gerenciamento de certificado da **Segurança**, dê entrada com o nome do certificado, consulte a seu lugar, e clique o **arquivo da transferência de arquivo pela rede**:

2. Transfira arquivos pela rede o certificado de todos os server do VCS. Faça isto em cada server CUCM que se comunicará com o VCS; este é tipicamente todos os Nós que estão dirigindo o serviço do CallManager.

Conexão do SORVO

Uma vez que os Certificados são validados e ambos os sistemas se confiam, configurar a zona vizinha no VCS e no tronco do SORVO em CUCM. Veja o gerente das comunicações unificadas de Cisco do Cisco TelePresence com o guia de distribuição do VCS de Cisco (tronco do SORVO) para detalhes deste procedimento.

Verificar

Confirme que a conexão do SORVO é ativa na zona vizinha no VCS:

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Gerente das comunicações unificadas de Cisco do Cisco TelePresence com o guia de distribuição do VCS de Cisco (tronco do SORVO)
- Guia de administrador do servidor de uma comunicação de vídeo do Cisco TelePresence
- Criação e uso do certificado do Cisco TelePresence com o guia de distribuição do VCS de Cisco
- Guia de Administração do sistema operacional das comunicações unificadas de Cisco
- Guia da administração do gerenciador das comunicações unificadas de Cisco
- Suporte Técnico e Documentação - Cisco Systems