Gerar CSR para certificados de terceiros e fazer o download de certificados desencadeados para o WLC

Índice

Introdução

Este documento explica como gerar uma solicitação de assinatura de certificado (CSR) a fim obter um certificado da terceira e como transferir um certificado soltado a um controlador do Wireless LAN (WLAN) (WLC).

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento de como configurar o WLC, o Access point de pouco peso (REGAÇO), e o cartão do cliente Wireless para a operação básica
- Conhecimento de como usar o pedido do OpenSSL para o Secure Socket Layer (SSL)

Componentes Utilizados

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

- Cisco 4400 WLC que executa a versão de firmware 4.2.61.0

- Pedido do OpenSSL para Microsoft Windows**Nota:** O OpenSSL 0.9.8 é exigido porque o WLC não apoia atualmente o OpenSSL 1.0.
- Ferramenta do registro que é específica ao Certification Authority (CA) da terceira

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.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

À revelia, os WLC usam um certificado auto-assinado acessório SSL. Os WLC usam este certificado SSL em uma destas situações:

- Quando os clientes tentarem conectar à rede de WLAN com o uso da autenticação da Web SSL-baseada
- Quando um usuário tentar entrar ao WLC com uso de HTTP seguro (HTTPS) (autenticação de WebAdmin)

Em qualquer dos casos, na primeira tentativa de alcançar o WLC, você pode receber uma alerta de segurança do web browser que olhe como esta:

Você é alertado aceitar o certificado do WLC porque os clientes não têm um certificado do root confiável para o certificado que é instalado no WLC. O certificado SSL no WLC não está na lista de Certificados que o sistema de cliente confia. Há duas maneiras de parar a geração desta janela pop-up da alerta de segurança do web browser:

- Use o certificado auto-assinado SSL no WLC e configurar as estações do cliente para aceitar o certificado.Inclua o certificado auto-assinado no WLC na lista de Certificados que são confiados na estação do cliente.
- Gerencia um CSR e instale um certificado que seja assinado por uma fonte (CA da terceira) para que os clientes já têm os Certificados do root confiável instalados, como Verisign.Você pode fazer este autônomo do WLC com o uso de um programa como o OpenSSL. Refira o projeto openSSL para obter mais informações sobre do OpenSSL.

Este documento explica como gerar um CSR para um certificado da terceira parte e como transferir um certificado soltado da autenticação da Web ao WLC.

Apoio para o certificado acorrentado

As versões de software WLC mais cedo do que 5.1.151.0 não apoiam Certificados acorrentados. Use uma da ação alternativa destas opções esta edição:

- Adquira um certificado soltado de CA, assim que significa que a raiz de assinatura está confiada.
- Tenha todos os certificados de raiz intermediários válidos de CA, confiados ou não-confiável,

instalado no cliente.

Com versão 5.1.151.0 e mais tarde, o apoio WLC acorrentou Certificados para a autenticação da Web. Os Certificados da autenticação da Web podem ser qualquens um:

- Acorrentado
- Soltado
- Gerado automaticamente

Consulte para gerar o CSR para Certificados da terceira e para transferir Certificados acorrentados ao WLC para obter informações sobre de como usar Certificados acorrentados no WLC.

CSR

Um certificado é um documento eletrónico que você use a fim identificar um server, uma empresa, ou alguma outra entidade e associar essa identidade com uma chave pública.

Os CA são as entidades que validam identidades e emitem Certificados. O certificado que CA emite ligamentos uma chave pública particular ao nome da entidade que o certificado identifica (como o nome de um server ou de um dispositivo). Somente a chave pública que o certificado certifica trabalhos com a chave privada correspondente que é possuída pela entidade que o certificado identifica. Os Certificados ajudam a impedir o uso de chaves públicas falsificadas para a personificação.

Um CSR é uma mensagem que um candidato envie a CA a fim aplicar para um certificado de identidade digital. Geralmente, uma empresa da terceira de CA, como confia ou Verisign, exige um CSR antes que a empresa possa criar um certificado digital.

A geração CSR é independente do dispositivo em que você planeia instalar um certificado externo. Assim um CSR e um arquivo-chave privado podem ser gerados em todo o Windows ou máquina Unix individual. A geração CSR não é interruptor-dependente ou dispositivo-dependente neste caso.

Porque o WLC não gerencie um CSR, você deve usar um aplicativo de terceiros tal como o OpenSSL a fim gerar um CSR para o WLC.

A seção gerencie um CSR discute os comandos que você deve emitir no aplicativo do OpenSSL a fim gerar uma chave privada e o CSR.

Termine estas etapas a fim obter um certificado da terceira de CA:

1. Gerencia um par privado/chave pública.
2. Com uso da chave pública, gerencia um CSR.
3. Submeta o CSR a CA.
4. Recupere o certificado que CA produz.
5. Combine o certificado e a chave privada em um arquivo do pkcs12.
6. Converta o arquivo do pkcs12 a um arquivo de codificação do Privacy Enhanced Mail (PEM).
7. Transfira o certificado da terceira novo (arquivo do .pem) no WLC.

Gerencia um CSR

Termine estas etapas a fim gerar um CSR e submeter o CSR a CA da terceira:

1. Instale e abra o aplicativo do OpenSSL.**Nota:** O OpenSSL 0.9.8 é exigido porque o WLC não apoia atualmente o OpenSSL 1.0.Em Windows, à revelia, openssl.exe é ficado situado em c:\openssl\bin.
2. Emita este comando:`OpenSSL>`**`req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem`** **Nota:** Os WLC apoiam um tamanho chave máximo de **2048** bit.Depois que você emite o comando, há uma alerta para alguma informação: nome do país, estado, cidade, e assim por diante.
3. Forneça a informação requerida.A maioria de informação importante que você precisa de fornecer corretamente é o Common Name. Assegure-se de que o nome de host que é usado para criar o certificado (Common Name) combine a entrada de nome de host do Domain Name System (DNS) para o IP da interface virtual no WLC e que o nome existe realmente no DNS também. Também, depois que você faz a mudança à interface de VIP, você deve recarregar o sistema para que esta mudança tome o efeito.**Nota:** O nome de host DNS deve ser dado entrada com no WLC sob **relações > edita** para a interface virtual. Isto está usado para verificar a fonte de Certificados quando o AUTH da Web é permitido. Recarregue o controlador para mandar esta mudança tomar o efeito.Depois que você fornece todos os detalhes exigidos, você termina acima com dois arquivos:uma chave privada nova que tenha o nome mykey.pemum CSR que tenha o nome myreq.pemEstes arquivos são armazenados no diretório padrão onde o OpenSSL é instalado (c:\openssl\bin, neste caso). O arquivo myreq.pem é o arquivo que contém a informação CSR. Esta informação deve ser submetida a CA da terceira de modo que CA da terceira possa gerar um certificado digital. Está aqui o exemplo de saída de comando quando você emite este comando com o uso do aplicativo do OpenSSL:`OpenSSL>`**`req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem`** `Loading 'screen' into random state - done Generating a 1024 bit RSA private key .....++++++ .....++++++ writing new private key to 'mykey.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]:`**`US`** `State or Province Name (full name) [Some-State]:`**`CA`** `Locality Name (eg, city) []:`**`San Jose`** `Organization Name (eg, company) [Internet Widgits Pty Ltd]:`**`ABC`** `Organizational Unit Name (eg, section) []:`**`CDE`** `Common Name (eg, YOUR name) []:`**`XYZ.ABC`** `Email Address []:`**`Test@abc.com`** `Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:`**`Test123`** `An optional company name []: OpenSSL>` **Nota:** Recorde a senha do desafio e preserve o arquivo-chave. Muito provavelmente, você precisará a senha quando você importa digitalmente o certificado assinado que CA da terceira envia (a menos que CA da terceira envia uma senha nova junto com o certificado digital que gerencie para você ou sua organização).
4. Agora que seu CSR está pronto, a cópia e cola a informação CSR em toda a ferramenta do registro de CA.A fim copiar e colar a informação no formulário do registro, abra o arquivo em um editor de texto que não adicione caráteres extra. Cisco recomenda que você usa o Microsoft Notepad ou o UNIX vi. Refira o Web site de CA da terceira para obter mais informações sobre de como submeter o CSR através da ferramenta do registro.Depois que você submete o CSR a CA da terceira, CA da terceira digitalmente assina o certificado e envia para trás o certificado assinado através do email.
5. Copie a informação do certificado assinado que você recebe para trás de CA em um arquivo.Este exemplo nomeia o arquivo CA.pem.
6. Combine o certificado CA.pem com a chave privada, e converta então o arquivo a um

arquivo do .pem.Emita este comando no aplicativo do OpenSSL:`openssl>`**`pkcs12 -export -in CA.pem -inkey mykey.pem -out CA.p12 -clcerts -passin pass:check123 -passout pass:check123`**
`!--- This command should be on one line.` `openssl>`**`pkcs12 -in CA.p12 -out final.pem -passin pass:check123 -passout pass:check123`** **Nota:** Neste comando, você deve incorporar uma senha para os parâmetros **`- passin`** e **`- passout`**. A senha que é configurada para **`-`** parâmetro do **`passout`** deve combinar o parâmetro do **`certpassword`** que é configurado no WLC. Neste exemplo, a senha que é configurada para **`- passin`** e **`- os`** parâmetros do **`passout`** são **check123**. Etapa 4 do procedimento na transferência o certificado da terceira à seção WLC deste documento discute a configuração do parâmetro do **`certpassword.O final.pem é o`** arquivo que é transferido através do TFTP a Cisco WLC.Agora que você tem o certificado de CA da terceira, você precisa de transferir o certificado ao WLC.

Transfira o certificado da terceira ao WLC

Use um servidor TFTP a fim carregar o certificado novo. Siga estas diretrizes para o uso do TFTP:

- Se você carrega o certificado através da porta do serviço, o servidor TFTP deve estar na mesma sub-rede como o WLC porque a porta do serviço não é roteável. Contudo, se você carrega o certificado através da porta de rede do sistema de distribuição (DS), o servidor TFTP pode estar em toda a sub-rede.
- O servidor TFTP não pode ser executado no mesmo computador que o Sistema de controle sem fio da Cisco (WCS) porque o WCS e o servidor TFTP usam a mesma porta de comunicação.

Termine estas etapas a fim carregar um certificado externamente gerado HTTPS:

1. Mova o arquivo final.pem para o diretório padrão em seu servidor TFTP.
2. No comando line interface(cli), emita o **comando transfer download start** a fim ver os ajustes atuais da transferência, e incorpore **n na** alerta.Aqui está um exemplo:`>`**`transfer download start`** `Mode..... TFTP Data Type..... Admin Cert TFTP Server IP..... xxx.xxx.xxx.xxx TFTP Path..... <directory path> TFTP Filename..... Are you sure you want to start? (y/n)` **`n`** `Transfer Canceled`
3. Emita estes comandos a fim mudar os ajustes da transferência:`>`**`transfer download mode tftp`** `>`**`transfer download datatype webauthcert`** `>`**`transfer download serverip`** *`<TFTP server IP address>`* `>`**`transfer download path`** *`<absolute TFTP server path to the update file>`* `>`**`transfer download filename`** *`final.pem`*
4. Incorpore a senha para o arquivo do .pem de modo que o sistema operacional possa decifrar a chave e o certificado SSL.`>`**`transfer download certpassword`** *`password`* `>Setting password to` *`password`* **Nota:** Seja certo que o **`certpassword`** é o mesmo que **`- a`** senha do parâmetro do **`passout`** que pisa 6 da geração uma seção CSR discute. Neste exemplo, o **`certpassword`** deve ser **check123**.
5. Emita o **comando transfer download start** a fim ver os ajustes actualizados. Incorpore então **y no** alerta a fim confirmar os ajustes atuais da transferência e começar a transferência do certificado e da chave.Aqui está um exemplo:`(Cisco Controller) >`**`transfer download start`** `Mode..... TFTP Data Type..... Admin Cert TFTP Server IP..... 172.16.1.1 TFTP Packet Timeout..... 6 TFTP Max Retries..... 10 TFTP Path..... c:\OpenSSL\bin/ TFTP`

```
Filename.................................. final.pem This may take some time. Are you
sure you want to start? (y/N) y TFTP Webadmin cert transfer starting. Certificate
installed. Reboot the switch to use new certificate.
```
Nota: A fim instalar um certificado da terceira para a autenticação (admin) administrativa (para um usuário que tente entrar ao WLC com uso do HTTPS), mude o tipo de dados ao **webadmincert no** comando do **datatype da transferência de transferência**, e repita etapas 3 com 5 deste procedimento.

6. Emita este comando a fim permitir o HTTPS:`>config network secureweb enable`
7. Salvar o certificado SSL, chave, e fixe a senha da Web ao NVRAM de modo que suas mudanças sejam retidas através das repartições.`>save config Are you sure you want to save? (y/n) y Configuration Saved!`
8. Recarregue o controlador.`>reset system Are you sure you would like to reset the system? (y/n) y System will now restart! The controller reboots.` **Nota:** Se um certificado é instalado já, o procedimento para transferir um novo apaga velho.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Você pode usar o **comando summary do certificado da mostra no** WLC a fim verificar se o WLC usa o certificado da terceira como esperado. Aqui está um exemplo:

```
(Cisco Controller) >show certificate summary Web Administration Certificate.................
3rd Party Web Authentication Certificate.................. 3rd Party Certificate compatibility
mode:.................. off
```
A saída confirma que um certificado da terceira está usado como o certificado da administração de web e o certificado da autenticação da Web.

A próxima vez que isso que um usuário tenta entrar à rede de WLAN com uso da autenticação da Web SSL-baseada, o usuário não está alertado aceitar uma alerta de segurança da Web, contanto que o certificado da terceira que está instalado no WLC está na lista de CA confiados que o navegador cliente apoia.

Troubleshooting

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Você pode usar o **comando debug pm pki enable no** WLC. Execute o comando quando você instala o certificado no WLC.

Sempre que todas as transferências a ou do controlador ocorrem, é útil girar sobre **transferência debugar todo o comando enable** e tornar a colocar em funcionamento transferência a fim ver os detalhes do que ocorreu. Transferências podem falhar no trânsito (o número apropriado de bit ou de bytes não se move do server para o controlador), ou uma vez que o arquivo obtém lá, os índices são um ou outro ilegíveis ao controlador ou não são encontrados para ser apropriados para a função desejada.

Informações Relacionadas

- Atualização do software do Wireless LAN Controller (WLC)
- Gerencia o CSR para Certificados da terceira e transfira Certificados acorrentados ao WLC
- Perguntas Frequentes de Troubleshooting de Controladoras Wireless LAN (WLC)
- Guia de Configuração da Cisco Wireless LAN Controller Release 4.0
- Suporte de produtos Wireless
- Projeto openSSL
- Suporte Técnico e Documentação - Cisco Systems