Contenido

Introducción

Este documento explica cómo generar un pedido de firma de certificado (CSR) para obtener un certificado de tercera persona con un sistema de control inalámbrico (WCS) y cómo cargar el certificado sobre el WCS.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo instalar y configurar el WCS para la operación básica
- Conocimiento de uno mismo-firmado y Certificados digitales, y otros mecanismos de seguridad relacionado con el Public Key Infrastructure (PKI)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 4.1.91.0 WCS**Nota:** La generación CSR que utiliza un WCS es solamente el comenzar soportado con la versión 4.1.91.0 WCS.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Pedido de firma de certificado (CSR)

Un certificado es un documento electrónico que usted utiliza para identificar un servidor, una compañía, o alguna otra entidad y asociar esa identidad a una clave pública.

Un certificado autofirmado es un certificado de identidad que es firmado por su propio creador. Es decir, la persona que creó el certificado también firmó apagado en su legitimidad.

Los Certificados se pueden uno mismo-firmar o se pueden atestiguar por una firma digital de un Certificate Authority (CA).

Los CA son las entidades que validan las identidades y publican los Certificados. El certificado que CA publica los lazos una clave pública determinada al nombre de la entidad que el certificado identifica, por ejemplo el nombre de un servidor o de un dispositivo. Solamente la clave pública que el certificado certifica los trabajos con la clave privada correspondiente poseyó al lado de la entidad que el certificado identifica. Los Certificados ayudan a prevenir el uso de las claves públicas falsas para la personificación.

Un CSR es un mensaje que un candidato envía a CA para solicitar un certificado de identidad digital. Antes de que se cree un CSR, el candidato primero genera un par clave, que mantiene la clave privada secreta. El CSR contiene la información que identifica el candidato, tal como a Directory Name (Nombre de directorio) en el caso de un certificado X.509, y la clave pública elegida por el candidato. La clave privada correspondiente no se incluye en el CSR, sino se utiliza para firmar digitalmente la petición entera.

El CSR se puede acompañar por otras credenciales o pruebas de la identidad requeridas por el Certificate Authority, y el Certificate Authority puede entrar en contacto al candidato para más información. En general, una compañía de tercera persona de CA, por ejemplo confía o Verisign, requiere un CSR antes de que la compañía pueda crear un certificado digital.

La generación CSR es independiente del dispositivo en el cual usted planea instalar un certificado externo. Por lo tanto, un CSR y un archivo de clave privado se pueden generar en cualquier máquina individual que soporte la generación CSR. La generación CSR no es Switch-dependiente o dispositivo-dependiente en este caso.

Este documento explica cómo generar el CSR para un certificado de tercera persona usando Cisco WCS.

Generación CSR usando un WCS

Los CSR en un WCS se pueden generar usando una herramienta disponible en el directorio de instalación WCS. Esta herramienta se llama **keyadmin.bat.**

Nota: Si el WCS está instalado en Linux, usted tendrá que utilizar la herramienta de **keyadmin.sh** disponible en **/opt/WCS4.1/bin/**. Este ejemplo muestra cómo generar un CSR e importar el

certificado firmado usando un WCS instalado en un servidor de Microsoft Windows 2003. El usuario raíz del WCS debe funcionar con este procedimiento para poder generar el certificado.

Complete estos pasos para acceder la herramienta:

1. Vaya al **comando prompt** disponible con Windows.
2. Va el directorio de instalación WCS, entonces al **compartimiento de la** carpeta.Aquí tiene un ejemplo:**C:\CD Program FilesC:\Program Files>CD WCS4.1C:\Program Files\WCS4.1> cd binC:\Program Files\WCS4.1\bin>**Esta carpeta tendrá la **herramienta keyadmin.bat** que se utiliza para generar el CSR.
3. Complete estos pasos para generar el CSR:Ingrese este comando:**keyadmin -newdn -csr genkey** `[csrFileName]`Esto genera una nuevos clave/par del certificado autofirmado, e hizo salir el CSR al archivo especificado. **- El** indicador del **newdn** lo hace indicar para los campos de nombre distintivo para el certificado. Es importante especificar el nombre de host final que será utilizado para acceder el WCS en el campo CN del DN para evitar las advertencias del navegador.Aquí tiene un ejemplo:**C:\Program Files\WCS4.1\bin>keyadmin -newdn -csr genkey C:\TEST\CSR-WCS.PEMThe WCS server is runningChanges will take affect on the next server restartEnter the domain name of the server: TS-WEBEnter the name of your organizational unit: ABCEnter the name of your organization: XYZEnter the name of your city or locality: SanjoseEnter the name of your state or province: CAEnter the two letter code for your country: USGenerating RSA keyConfiguring Apache server for keyWriting certificate signing request to C:\TEST\CSR-WCS.PEM**Una vez que se ejecuta el comando, la información CSR se genera y se escribe al archivo.La información CSR parece esto:**C:\Program Files\WCS4.1\bin>keyadmin -newdn -csr genkey C:\TEST\CSR-WCS.PEMThe WCS server is runningChanges will take affect on the next server restartEnter the domain name of the server: TS-WEBEnter the name of your organizational unit: ABCEnter the name of your organization: XYZEnter the name of your city or locality: SanjoseEnter the name of your state or province: CAEnter the two letter code for your country: USGenerating RSA keyConfiguring Apache server for keyWriting certificate signing request to C:\TEST\CSR-WCS.PEM**Ahora que su CSR está listo, la copia y pega la información CSR en cualquier herramienta de la inscripción de CA.Para copiar y pegar la información en la forma de la inscripción, abra el archivo en un editor de textos que no agregue los caracteres adicionales. Cisco recomienda que usted utiliza el Bloc de notas de Microsoft o UNIX VI. refiere al sitio web de CA de tercera persona para más información sobre cómo someter el CSR a través de la herramienta de la inscripción.Después de que usted someta el CSR a CA de tercera persona, CA de tercera persona firma digitalmente el certificado y devuelve el certificado firmado vía el correo electrónico.Una vez que usted consigue detrás el certificado firmado del CA, usted puede instalarlo para substituir el certificado autofirmado original ingresando este comando:**keyadmin importsignedcert** `[certFileName]`El certificado y la clave se salvan en **C:\ProgramFiles\WCS4.1\webnms\apache\conf\ssl.crt**.El certificado debe ser una certificación firmada X.509 en el formato PEM, y debe hacer juego la clave privada que fue generada originalmente por el comando del **genkey** (véase el paso 1). Por lo tanto, si usted genera una clave otra vez antes de que usted importe el certificado, rechazará el certificado.

Importe una clave/un par preexistentes del certificado al WCS

El WCS también tiene disposiciones para importar una clave/un par preexistentes del certificado. Para realizar esto, ingrese este comando:

keyadmin importkey *[keyFileName] [certFileName]*

La clave debe ser una clave privada PEM-codificada RSA con una línea con la cual comience

COMIENCEN LA CLAVE PRIVADA RSA, o puede ser una clave privada PEM-codificada RSA en el formato PKCS8 con una línea con la cual comience COMIENCEN LA CLAVE PRIVADA. En ambos casos, la clave no debe ser contraseña protegida.

El certificado debe ser un certificado PEM-codificado X.509 que hace juego la clave.

Importe un certificado de servidor con los CA intermedios

Si el certificado de servidor SSL es firmado por CA intermedio, para aseegurarse que el WCS devuelve el llavero lleno de CA, usted necesita combinar el certificado de servidor, los CA intermedios y certificado raíz CA en un nuevo certificado PEM:

keyadmin importkey *[keyFileName] [certFileName]*
Este nuevo archivo de certificado PEM es el [certFileName] que se utilizará con los comandos:

keyadmin importkey *[keyFileName] [certFileName]*

Verificación

Complete estos pasos para verificar si la configuración trabaja como se esperaba:

1. Después de que usted importe el certificado firmado encendido al WCS, recomience el WCS para que los cambios tomen el efecto.
2. Acceda el WCS a través del buscador Web.Si el certificado firmado es válido y tiene un Domain Name que corresponde con, el usuario debe ir a la derecha a la página de registro sin el problema con el diálogo amonestador móvil del certificado.

Troubleshooting

La herramienta Keyadmin.bat no generará el CSR adentro instala el directorio

Cuando **keyadmin.bat** se realiza en el WCS **\ el directorio BIN** en Windows, este error aparece:

```
Generating RSA keyConfiguring Apache server for keyWriting certificate signing request toError
generating key java.security.KeyStoreException: Could not create CSRC:\Program Files\WCS4.x\bin>
```

Para resolver este problema, defina un nombre de fichero en un cierto otro directorio además del directorio de instalación del WCS. Aquí tiene un ejemplo:

```
C:\Program Files\WCS4.2.81.0\bin>keyadmin -newdn -csr genkey C:\TEST\CSR-WCS.PEMThe WCS server
is runningChanges will take affect on the next server restartEnter the domain name of the
server: ciscoEnter the name of your organizational unit: ciscoEnter the name of your
organization: ciscoEnter the name of your city or locality: SJEnter the name of your state or
province: CAEnter the two letter code for your country: USGenerating RSA keyConfiguring Apache
server for key\Writing certificate signing request to C:\TEST\CSR-WCS.PEM
```

Información Relacionada

- Generación del pedido de firma de certificado (CSR) para un certificado de tercera persona en un controlador de WLAN (WLC)
- El resolver problemas inalámbrico del sistema de control
- Página de Soporte de Red Inalámbrica

- Soporte Técnico y Documentación - Cisco Systems