# Cómo establecer y configurar una autoridad de certificación (CA) en Ubuntu 22.04

# Prerrequisitos:

Para completar este tutorial, necesitará acceso a un servidor Ubuntu 22.04 para alojar su servidor CA. Deberá configurar un usuario no root con privilegios sudo antes de comenzar esta guía. Puede seguir la guía de configuración inicial del servidor Ubuntu 22.04 para configurar un usuario con los permisos adecuados. El tutorial vinculado también configurará un firewall, que se supone que está implementado a lo largo de esta guía.

Este servidor se denominará servidor CA en este tutorial.

Asegúrese de que el servidor CA sea un sistema independiente. Solo se utilizará para importar, firmar y revocar solicitudes de certificados. No debería ejecutar ningún otro servicio e, idealmente, estará fuera de línea o completamente cerrado cuando no esté trabajando activamente con su CA.

**Nota**: La última sección de este tutorial es opcional si desea obtener información sobre cómo firmar y revocar certificados. Si elige completar esos pasos de práctica, necesitará un segundo servidor Ubuntu 22.04 o también puede usar su propia computadora Linux local con Ubuntu o Debian, o distribuciones derivadas de cualquiera de ellos.

# Step 1 — Instalando Easy-RSA

La primera tarea de este tutorial es instalar el conjunto de scripts easy-rsa en su servidor CA. easy-rsa es una herramienta de administración de la autoridad de certificación que usará para generar una clave privada y un certificado raíz público, que luego usará para firmar solicitudes de clientes y servidores que dependerán de su CA.

Inicie sesión en su servidor CA como el usuario sudo no raíz que creó durante los pasos de configuración inicial y ejecute lo siguiente:sudo apt update

$ sudo apt install easy-rsa

Se le pedirá que descargue el paquete y lo instale. Presione y para confirmar que desea instalar el paquete.

En este punto, tiene todo lo que necesita configurado y listo para usar Easy-RSA. En el siguiente paso, creará una infraestructura de clave pública y luego comenzará a construir su autoridad de certificación.

# Step 2 — Preparación de un directorio de infraestructura de clave pública

Ahora que ha instalado easy-rsa, es el momento de crear una infraestructura de clave pública (PKI) básica en el servidor de CA. Asegúrese de seguir conectado como su usuario no root y cree un directorio easy-rsa. Asegúrese de no usar sudo para ejecutar ninguno de los siguientes comandos, ya que su usuario normal debe administrar e interactuar con la CA sin privilegios elevados.

$ mkdir ~/easy-rsa

Esto creará un nuevo directorio llamado easy-rsa en su carpeta de inicio. Usaremos este directorio para crear enlaces simbólicos que apunten a los archivos del paquete easy-rsa que instalamos en el paso anterior. Estos archivos se encuentran en la carpeta /usr/share/easy-rsa del servidor CA.

Cree los enlaces simbólicos con el comando ln:

ln -s /usr/share/easy-rsa/\* ~/easy-rsa/

Nota: mientras que otras guías pueden indicarle que copie los archivos del paquete easy-rsa en su directorio PKI, este tutorial adopta un enfoque de enlace simbólico. Como resultado, cualquier actualización del paquete easy-rsa se reflejará automáticamente en los scripts de su PKI.

Para restringir el acceso a su nuevo directorio PKI, asegúrese de que solo el propietario pueda acceder mediante el comando chmod:

chmod 700 /home/sammy/easy-rsa

Finally, initialize the PKI inside the easy-rsa directory:

cd ~/easy-rsa

./easyrsa init-pki

Output

init-pki complete; you may now create a CA or requests.

Your newly created PKI dir is: /home/sammy/easy-rsa/pki

Después de completar esta sección, tiene un directorio que contiene todos los archivos necesarios para crear una Autoridad de certificación. En la siguiente sección, creará la clave privada y el certificado público para su CA.

# Step 3 — Creando un certificado para la entidad Certificadora (Certificate Authority)

Antes de que pueda crear la clave privada y el certificado de su CA, debe crear y completar un archivo llamado vars con algunos valores predeterminados. Primero ingresará al directorio easy-rsa, luego creará y editará el archivo vars con nano o su editor de texto preferido:

cd ~/easy-rsa

nano vars

Una vez abierto el archivo, pegue las siguientes líneas y edite cada valor resaltado para reflejar la información de su propia organización. La parte importante aquí es asegurarse de no dejar ninguno de los valores en blanco:

~/easy-rsa/vars

set\_var EASYRSA\_REQ\_COUNTRY "ES"

set\_var EASYRSA\_REQ\_PROVINCE "Madrid"

set\_var EASYRSA\_REQ\_CITY "Madrid"

set\_var EASYRSA\_REQ\_ORG "Adams"

set\_var EASYRSA\_REQ\_EMAIL "admin@example.com"

set\_var EASYRSA\_REQ\_OU "Academia"

set\_var EASYRSA\_ALGO "ec"

set\_var EASYRSA\_DIGEST "sha512"

Cuando haya terminado, guarde y cierre el archivo. Si está utilizando nano, puede hacerlo presionando CTRL+X, luego Y y ENTER para confirmar. Ahora está listo para construir su CA.

Para crear el par de claves raíz pública y privada para su autoridad de certificación, ejecute el comando ./easy-rsa nuevamente, esta vez con la opción build-ca:

$ ./easyrsa build-ca

En el resultado, verá algunas líneas sobre la versión de OpenSSL y se le pedirá que ingrese una frase de contraseña para su par de claves. Asegúrese de elegir una frase de contraseña segura y anótela en un lugar seguro. Deberá ingresar la frase de contraseña cada vez que necesite interactuar con su CA, por ejemplo, para firmar o revocar un certificado.

También se le pedirá que confirme el nombre común (CN) de su CA. El CN es el nombre que se usa para referirse a esta máquina en el contexto de la Autoridad de certificación. Puede ingresar cualquier cadena de caracteres para el Nombre común de la CA, pero por razones de simplicidad, presione ENTER para aceptar el nombre predeterminado.

Output

. . .

Enter New CA Key Passphrase:

Re-Enter New CA Key Passphrase:

. . .

Common Name (ej:su usuario, host, server name) [Easy-RSA CA]:

Se completó la creación de CA y ahora puede importar y firmar solicitudes de certificado.

Su nuevo archivo de certificado de CA para publicación se encuentra en:

/home/sammy/easy-rsa/pki/ca.crt

Nota: si no desea que se le solicite una contraseña cada vez que interactúa con su CA, puede ejecutar el comando build-ca con la opción nopass, así:

$ ./easyrsa build-ca nopass

Ahora tiene dos archivos importantes, ~/easy-rsa/pki/ca.crt y ~/easy-rsa/pki/private/ca.key, que conforman los componentes público y privado de una autoridad de certificación.

ca.crt es el archivo de certificado público de la CA. Los usuarios, servidores y clientes utilizarán este certificado para verificar que forman parte de la misma red de confianza. Cada usuario y servidor que use su CA necesitará tener una copia de este archivo. Todas las partes confiarán en el certificado público para asegurarse de que alguien no se esté haciendo pasar por un sistema y realice un ataque Man-in-the-middle.

ca.key es la clave privada que utiliza la CA para firmar certificados para servidores y clientes. Si un atacante obtiene acceso a su CA y, a su vez, a su archivo ca.key, deberá destruir su CA. Esta es la razón por la que su archivo ca.key solo debe estar en su máquina CA y que, idealmente, su máquina CA debe mantenerse fuera de línea cuando no esté firmando solicitudes de certificados como medida de seguridad adicional.

Con eso, su CA está en su lugar y está lista para usarse para firmar solicitudes de certificados y revocar certificados.

# Step 4 — Distribuyendo el certificado de la Entidad Certificadora (Authority’s Public Certificate)

Ahora su CA está configurada y lista para actuar como una raíz de confianza para cualquier sistema que desee configurar para usarla. Puede agregar el certificado de CA a sus servidores OpenVPN, servidores web, servidores de correo, etc. Cualquier usuario o servidor que necesite verificar la identidad de otro usuario o servidor en su red debe tener una copia del archivo ca.crt importado en el almacén de certificados de su sistema operativo.

Para importar el certificado público de la CA a un segundo sistema Linux como otro servidor o una computadora local, primero obtenga una copia del archivo ca.crt de su servidor de la CA. Puede usar el comando cat para generarlo en una terminal y luego copiarlo y pegarlo en un archivo en la segunda computadora que está importando el certificado. También puede usar herramientas como scp, rsync para transferir el archivo entre sistemas. Sin embargo, usaremos copiar y pegar con nano en este paso, ya que funcionará en todos los sistemas.

Como su usuario no root en el servidor CA, ejecute el siguiente comando:

cat ~/easy-rsa/pki/ca.crt

Habrá una salida en su terminal que es similar a la siguiente:

Output

-----BEGIN CERTIFICATE-----

MIIDSzCCAjOgAwIBAgIUcR9Crsv3FBEujrPZnZnU4nSb5TMwDQYJKoZIhvcNAQEL

BQAwFjEUMBIGA1UEAwwLRWFzeS1SU0EgQ0EwHhcNMjAwMzE4MDMxNjI2WhcNMzAw

. . .

. . .

-----END CERTIFICATE-----

Copie todo, incluidas las líneas -----BEGIN CERTIFICATE----- y -----END CERTIFICATE----- y los guiones.

En su segundo sistema Linux, use nano o su editor de texto preferido para abrir un archivo llamado /tmp/ca.crt:

$ nano /tmp/ca.crt

Pegue el contenido que acaba de copiar del servidor CA en el editor. Cuando haya terminado, guarde y cierre el archivo. Si está utilizando nano, puede hacerlo presionando CTRL+X, luego Y y ENTER para confirmar.

Ahora que tiene una copia del archivo ca.crt en su segundo sistema Linux, es hora de importar el certificado al almacén de certificados de su sistema operativo.

En sistemas basados ​​en Ubuntu y Debian, ejecute los siguientes comandos como su usuario no root para importar el certificado:

Distribuciones derivadas de Ubuntu y Debiansudo

cp /tmp/ca.crt /usr/local/share/ca-certificates/

sudo update-ca-certificates

Now your second Linux system will trust any certificate that has been signed by the CA server.

Nota: si está utilizando su CA con servidores web y utiliza Firefox como navegador, deberá importar el certificado público ca.crt a Firefox directamente. Firefox no utiliza el almacén de certificados del sistema operativo local.

Si está utilizando su CA para integrarse con un entorno de Windows o computadoras de escritorio, consulte la documentación sobre cómo usar certutil.exe para instalar un certificado de CA.

Si está utilizando este tutorial como requisito previo para otro tutorial, o está familiarizado con cómo firmar y revocar certificados, puede detenerse aquí. Si desea obtener más información sobre cómo firmar y revocar certificados, la siguiente sección opcional explicará cada proceso en detalle.

Si desea practicar y obtener más información sobre cómo firmar solicitudes de certificados y cómo revocar certificados, estas secciones opcionales explicarán cómo funcionan ambos procesos.

## (Opcional) — Creación y firma de una solicitud de certificado de práctica

Ahora que tiene una CA lista para usar, puede practicar la generación de una clave privada y una solicitud de certificado para familiarizarse con el proceso de firma y distribución.

Una solicitud de firma de certificado (CSR) consta de tres partes: una clave pública, que identifica información sobre el sistema solicitante, y una firma de la solicitud en sí, que se crea utilizando el clave privada de la parte solicitante. La clave privada se mantendrá en secreto y se utilizará para cifrar información que cualquier persona con el certificado público firmado puede descifrar.

Los siguientes pasos se ejecutarán en su segundo sistema Ubuntu o Debian, o en una distribución derivada de cualquiera de ellos. Puede ser otro servidor remoto o una máquina Linux local como una computadora portátil o de escritorio. Dado que easy-rsa no está disponible de forma predeterminada en todos los sistemas, utilizaremos la herramienta openssl para crear una clave privada y un certificado de práctica.

openssl generalmente se instala de forma predeterminada en la mayoría de las distribuciones de Linux, pero solo para estar seguro, ejecute lo siguiente en su sistema:

$ sudo apt update

$ sudo apt install openssl

Cuando se le solicite que instale openssl, ingrese y para continuar con los pasos de instalación. Ahora está listo para crear una práctica CSR con openssl.

El primer paso que debe completar para crear una CSR es generar una clave privada. Para crear una clave privada usando openssl, cree un directorio de práctica-csr y luego genere una clave dentro de él. Realizaremos esta solicitud para un servidor ficticio llamado sammy-server, en lugar de crear un certificado que se utilice para identificar a un usuario u otra CA

.$mkdir ~/practice-csr

$ cd ~/practice-csr

$ openssl genrsa -out sammy-server.key

Ahora que tiene una clave privada, puede crear una CSR correspondiente, nuevamente usando la utilidad openssl. Se le pedirá que complete una serie de campos como País, Estado y Ciudad. Puede ingresar un . si desea dejar un campo en blanco, pero tenga en cuenta que si se tratara de una CSR real, es mejor utilizar los valores correctos para su ubicación y organización:

$openssl req -new -key sammy-server.key -out sammy-server.req

Output

. . .

-----

Country Name (2 letter code) [XX]:ES

State or Province Name (full name) []:Madrid

Locality Name (eg, city) [Default City]:Madrid

Organization Name (eg, company) [Default Company Ltd]:Adams

Organizational Unit Name (eg, section) []:Academia

Common Name (eg, your name or your server's hostname) []:sammy-server

Email Address []:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

Si desea agregar automáticamente esos valores como parte de la invocación de openssl en lugar de a través del mensaje interactivo, puede pasar el argumento -subj a OpenSSL. Asegúrese de editar los valores resaltados para que coincidan con la ubicación de su práctica, la organización y el nombre del servidor:

$ openssl req -new -key sammy-server.key -out server.req -subj \

/C=ES/ST=Madrid/L=Madrid/O=Adams/OU=Academia/CN=sammy-server

Para verificar el contenido de una CSR, puede leer un archivo de solicitud con openssl y examinar los campos dentro:

openssl req -in sammy-server.req -noout -subject

Output

subject=C = ES, ST = Madrid, L = Madrid, O = Adams, OU =Academia, CN = sammy-server

Una vez que esté satisfecho con el tema de su solicitud de certificado de práctica, copie el archivo sammy-server.req en su servidor CA usando scp:

scp sammy-server.req sammy@your\_ca\_server\_ip:/tmp/sammy-server.req

En este paso, generó una solicitud de firma de certificado para un servidor ficticio llamado sammy-server. En un escenario del mundo real, la solicitud podría provenir de algo así como un servidor web de prueba o desarrollo que necesita un certificado TLS para la prueba; o podría provenir de un servidor OpenVPN que solicita un certificado para que los usuarios puedan conectarse a una VPN. En el siguiente paso, procederemos a firmar la solicitud de firma del certificado utilizando la clave privada del servidor CA.

## (Optional) — Firmando una petición CSR

En el paso anterior, creó una solicitud de certificado de práctica y una clave para un servidor ficticio. Lo copió en el directorio /tmp en su servidor CA, emulando el proceso que usaría si tuviera clientes o servidores reales que le enviaran solicitudes de CSR que deben firmarse.

Continuando con el escenario ficticio, ahora el servidor CA necesita importar el certificado de práctica y firmarlo. Una vez que la CA valida una solicitud de certificado y la retransmite a un servidor, los clientes que confían en la autoridad de certificación también podrán confiar en el certificado recién emitido.

Como estaremos operando dentro de la PKI de la CA donde está disponible la utilidad easy-rsa, los pasos de firma usarán la utilidad easy-rsa para facilitar las cosas, en lugar de usar el openssl directamente como lo hicimos en el ejemplo anterior.The first step to sign the fictional CSR is to import the certificate request using the easy-rsa script:

$ cd ~/easy-rsa

$ ./easyrsa import-req /tmp/sammy-server.req sammy-server

Output

. . .

La solicitud se ha importado con éxito con un nombre corto de: sammy-server

Ahora puede usar este nombre para realizar operaciones de firma en esta solicitud.

Ahora puede firmar la solicitud ejecutando el script easyrsa con la opción sign-req, seguido del tipo de solicitud y el nombre común que se incluye en la CSR. El tipo de solicitud puede ser cliente, servidor o ca. Como estamos practicando con un certificado para un servidor ficticio, asegúrese de usar el tipo de solicitud del servidor:$ ./easyrsa sign-req server sammy-server

En el resultado, se le pedirá que verifique que la solicitud proviene de una fuente confiable. Escriba sí y luego presione ENTER para confirmar esto:

Output

You are about to sign the following certificate.

Please check over the details shown below for accuracy. Note that this request

has not been cryptographically verified. Please be sure it came from a trusted

source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 825 days:

subject=

countryName = ES

stateOrProvinceName = Madrid

localityName = Madrid

organizationName = Adams

organizationalUnitName = Academia

commonName = sammy-server

Type the word 'yes' to continue, or any other input to abort.

Confirm request details: yes

. . .

Si encriptó su clave de CA, se le pedirá su contraseña en este punto.

Recibirá una salida como la siguiente:

Output

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

countryName :PRINTABLE:'US'

stateOrProvinceName :ASN.1 12:'New York'

localityName :ASN.1 12:'New York City'

organizationName :ASN.1 12:'DigitalOcean'

organizationalUnitName:ASN.1 12:'Community'

commonName :ASN.1 12:'sammy-server'

Certificate is to be certified until Jul 21 13:59:08 2024 GMT (825 days)

Write out database with 1 new entries

Data Base Updated

Certificado creado en: /home/sammy/easy-rsa/pki/issued/sammy-server.crt

Con esos pasos completados, ha firmado el CSR sammy-server.req utilizando la clave privada del servidor CA en

/home/sammy/easy-rsa/pki/private/ca.key.

El archivo sammy-server.crt resultante contiene la clave de cifrado pública del servidor de práctica, así como una nueva firma del servidor CA. El objetivo de la firma es decirle a cualquiera que confíe en la CA que también puede confiar en el certificado del servidor sammy.

Si esta solicitud fuera para un servidor real como un servidor web o un servidor VPN, el último paso en el servidor CA sería distribuir los nuevos archivos sammy-server.crt y ca.crt desde el servidor CA al servidor remoto que realizó el Solicitud de RSC:

scp pki/issued/sammy-server.crt sammy@your\_server\_ip:/tmp

scp pki/ca.crt sammy@your\_server\_ip:/tmp

En este punto, podrá usar el certificado emitido con algo como un servidor web, una VPN, una herramienta de administración de configuración, un sistema de base de datos o para fines de autenticación de clientes.

**(Optional) — Revoking a Certificate**

Ocasionalmente, es posible que deba revocar un certificado para evitar que un usuario o servidor lo use. Tal vez le robaron la computadora portátil a alguien, un servidor web se vio comprometido o un empleado o contratista abandonó su organización.

Para revocar un certificado, el proceso general sigue estos pasos:

Revocar el certificado con el comando ./easyrsa revoke client\_name

Generar el nuevo certificado con el comando ./easyrsa gen-crl

Transfiera el archivo crl.pem actualizado al servidor o servidores que dependen de su CA y, en esos sistemas, cópielo en el directorio o directorios requeridos para los programas que hacen referencia a él.

Reinicie cualquier servicio que use su CA y el archivo CRL.

Puede utilizar este proceso para revocar cualquier certificado que haya emitido anteriormente en cualquier momento. Repasaremos cada paso en detalle en las siguientes secciones, comenzando con el comando revoke.

## Revocación de un certificado

Para revocar un certificado, vaya al directorio easy-rsa en su servidor de CA:

cd ~/easy-rsa

A continuación, ejecute el script easyrsa con la opción de revocación, seguido del nombre del cliente que desea revocar. Siguiendo el ejemplo práctico anterior, el nombre común del certificado es sammy-server:

./easyrsa revoke sammy-server

Esto le pedirá que confirme la revocación ingresando sí:

Output

Please confirm you wish to revoke the certificate with the following subject:

subject=

commonName = sammy-server

Type the word 'yes' to continue, or any other input to abort.

Continue with revocation: yes

. . .

Revoking Certificate 8348B3F146A765581946040D5C4D590A

. . .

Tenga en cuenta el valor resaltado en la línea Certificado de revocación. Este valor es el número de serie único del certificado que se revoca. Si desea examinar la lista de revocación en el último paso de esta sección para verificar que el certificado está en ella, necesitará este valor.

Después de confirmar la acción, la CA revocará el certificado. Sin embargo, los sistemas remotos que dependen de la CA no tienen forma de comprobar si se ha revocado algún certificado. Los usuarios y servidores aún podrán usar el certificado hasta que la Lista de revocación de certificados (CRL) de la CA se distribuya a todos los sistemas que dependen de la CA.

En el siguiente paso, generará una CRL o actualizará un archivo crl.pem existente.

**Generación de una lista de revocación de certificados**

Ahora que ha revocado un certificado, es importante actualizar la lista de certificados revocados en su servidor CA. Una vez que tenga una lista de revocación actualizada, podrá saber qué usuarios y sistemas tienen certificados válidos en su CA.

Para generar una CRL, ejecute el comando easy-rsa con la opción

gen-crl estando en la carpeta ~/easy-rsa directory:

./easyrsa gen-crl

Si usó una frase de contraseña al crear su archivo ca.key, se le pedirá que la ingrese. El comando gen-crl generará un archivo llamado crl.pem, que contiene la lista actualizada de certificados revocados para esa CA.

A continuación, deberá transferir el archivo crl.pem actualizado a todos los servidores y clientes que dependen de esta CA cada vez que ejecute el comando gen-crl. De lo contrario, los clientes y los sistemas aún podrán acceder a los servicios y sistemas que usan su CA, ya que esos servicios necesitan conocer el estado revocado del certificado.

**Transferencia de una lista de revocación de certificado.**

Ahora que ha generado una CRL en su servidor de CA, debe transferirla a sistemas remotos que dependen de su CA. Para transferir este archivo a sus servidores, puede usar el comando scp.

Nota: Este tutorial explica cómo generar y distribuir una CRL manualmente. Si bien existen métodos más robustos y automatizados para distribuir y verificar listas de revocación como OCSP-Stapling, configurar esos métodos está más allá del alcance de este artículo.

Asegúrese de haber iniciado sesión en su servidor de CA como su usuario no raíz y ejecute lo siguiente, sustituyendo su propia IP de servidor o nombre DNS en lugar de your\_server\_ip:

scp ~/easy-rsa/pki/crl.pem [sammy@your\_server\_ip](mailto:sammy@your_server_ip):/tmp

Ahora que el archivo está en el sistema remoto, el último paso es actualizar cualquier servicio con la nueva copia de la lista de revocación.

**Actualización de servicios que admiten una CRL**

Enumerar los pasos que debe seguir para actualizar los servicios que utilizan el archivo crl.pem está fuera del alcance de este tutorial. En general, deberá copiar el archivo crl.pem en la ubicación que espera el servicio y luego reiniciarlo usando systemctl.

Una vez que haya actualizado sus servicios con el nuevo archivo crl.pem, sus servicios podrán rechazar conexiones de clientes o servidores que estén usando un certificado revocado.

**Examinando y verificando los contenidos de una CRL (Lista de revocación de certificados)**

Si desea examinar un archivo CRL, por ejemplo, para confirmar una lista de certificados revocados, use el siguiente comando openssl desde su directorio easy-rsa en su servidor CA:

cd ~/easy-rsa

openssl crl -in pki/crl.pem -noout -text

También puede ejecutar este comando en cualquier servidor o sistema que tenga instalada la herramienta openssl con una copia del archivo crl.pem. Por ejemplo, si transfirió el archivo crl.pem a su segundo sistema y desea verificar que el certificado del servidor sammy está revocado, puede usar un comando openssl como el siguiente, sustituyendo el número de serie que anotó anteriormente cuando revocó el certificado en lugar del resaltado aquí:

openssl crl -in /tmp/crl.pem -noout -text |grep -A 1 8348B3F146A765581946040D5C4D590A

Output

Serial Number: 8348B3F146A765581946040D5C4D590A

Revocation Date: Apr 18 14:00:37 2022 GMT

Observe cómo se usa el comando grep para verificar el número de serie único que anotó en el paso de revocación. Ahora puede verificar el contenido de su Lista de revocación de certificados en cualquier sistema que dependa de ella para restringir el acceso a usuarios y servicios.

# Conclusion

En este tutorial, creó una autoridad de certificación privada utilizando el paquete Easy-RSA en un servidor Ubuntu 22.04 independiente. Exploró cómo funciona el modelo de confianza entre las partes que dependen de la CA. También creó y firmó una solicitud de firma de certificado (CSR) para un servidor de práctica y luego aprendió cómo revocar un certificado. Finalmente, aprendió cómo generar y distribuir una Lista de revocación de certificados (CRL) para cualquier sistema que dependa de su CA para garantizar que los usuarios o servidores que no deben acceder a los servicios no puedan hacerlo.

Ahora puede emitir certificados para usuarios y usarlos con servicios como OpenVPN. También puede usar su CA para configurar servidores web de desarrollo y ensayo con certificados para proteger sus entornos que no son de producción. El uso de una CA con certificados TLS durante el desarrollo puede ayudar a garantizar que su código y entornos coincidan lo más posible con su entorno de producción.

Si desea obtener más información sobre cómo usar OpenSSL, nuestro tutorial OpenSSL Essentials: Trabajar con certificados SSL, claves privadas y CSR tiene mucha información adicional para ayudarlo a familiarizarse con los fundamentos de OpenSSL.