Gestión de certificados de seguridad

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

Tabla de contenidos

Gestión de certificados de seguridad

Puede configurar HTTPS en el servidor de Unified Manager para supervisar y gestionar los clústeres a través de una conexión segura.

Visualizar el certificado de seguridad HTTPS

Es posible comparar los detalles del certificado HTTPS con el certificado recuperado en el explorador para asegurarse de que la conexión cifrada del explorador con Unified Manager no se intercepte.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

La visualización del certificado permite verificar el contenido de un certificado regenerado o ver los nombres Alt (SAN) sujetos desde los que puede acceder a Unified Manager.

Paso

1. En el panel de navegación izquierdo, haga clic en **General** > **Certificado HTTPS**.

   El certificado HTTPS se muestra en la parte superior de la página

Si necesita ver información más detallada sobre el certificado de seguridad que la que aparece en la página Certificado HTTPS, puede ver el certificado de conexión en el explorador.

Descargar una solicitud de firma de certificación HTTPS

Puede descargar una solicitud de firma de certificación para el certificado de seguridad HTTPS actual para poder proporcionar el archivo a una entidad de certificación para firmar. Un certificado firmado por CA ayuda a evitar ataques de tipo "man in the middle" y proporciona una mejor protección de seguridad que un certificado autofirmado.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Certificado HTTPS**.
2. Haga clic en **Descargar la solicitud de firma de certificado HTTPS**.
3. Guarde la `<hostname>.csr` archivo.

Puede proporcionar el archivo a una entidad de certificación para firmar e instalar el certificado firmado.

Instalar una CA firmada y devolvió un certificado HTTPS

Puede cargar e instalar un certificado de seguridad después de que una entidad de certificación lo haya firmado y devuelto. El archivo que cargue e instale debe ser una

versión firmada del certificado autofirmado existente. Un certificado firmado por CA ayuda a evitar los ataques de tipo "man in the middle" y ofrece una mejor protección de seguridad que un certificado autofirmado.

Lo que necesitará

Debe haber completado las siguientes acciones:

- Descargó el archivo de solicitud de firma de certificado y lo firmó una entidad de certificación
- Se guardó la cadena de certificados en formato PEM
- Se incluyeron todos los certificados en la cadena, desde el certificado de servidor de Unified Manager hasta el certificado de firma raíz, incluidos los certificados intermedios presentes

Debe tener la función Administrador de aplicaciones.

Si la validez del certificado para el que se creó una CSR es superior a 397 días, la CA reducirá la validez a 397 días antes de firmar y devolver el certificado

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Certificado HTTPS**.
2. Haga clic en **instalar certificado HTTPS**.
3. En el cuadro de diálogo que aparece, haga clic en **elegir archivo…** para localizar el archivo que se va a cargar.
4. Seleccione el archivo y haga clic en **instalar** para instalarlo.

   Para obtener más información, consulte "Instalar un certificado HTTPS generado con herramientas externas".

Ejemplo de cadena de certificados

El siguiente ejemplo muestra cómo puede aparecer el archivo de cadena de certificados:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Instalar un certificado HTTPS generado con herramientas externas

Puede instalar certificados que están autofirmados o firmados por CA y que se generan con una herramienta externa como OpenSSL, BoringSSL o LetsEncrypt.

Debe cargar la clave privada junto con la cadena de certificados porque estos certificados son pares de claves pública-privada generados externamente. Los algoritmos de pares de claves permitidos son «'RSA'» y «'EC'». La opción **instalar certificado HTTPS** está disponible en la página certificados HTTPS de la sección General. El archivo que cargue debe tener el siguiente formato de entrada.

1. Clave privada del servidor que pertenece al host Active IQ Unified Manager
2. Certificado del servidor que coincide con la clave privada
3. Certificado de las CA en reverso hasta la raíz, que se utilizan para firmar el certificado anterior

Formato para cargar un certificado con un par de claves EC

Las curvas permitidas son «'prime256v1» y «slecp384r1». Ejemplo de certificado con un par de EC generado externamente:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Formato para cargar un certificado con un par de claves RSA

Los tamaños de claves permitidos del par de claves RSA que pertenece al certificado de host son 2048, 3072 y 4096. Certificado con un par de claves **RSA** generado externamente:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Una vez cargado el certificado, debe reiniciar la instancia de Active IQ Unified Manager para que los cambios se apliquen.

Comprueba la carga de certificados generados externamente

El sistema realiza comprobaciones mientras carga un certificado generado mediante herramientas externas. Si alguna de las comprobaciones falla, se rechaza el certificado. También se incluye una validación para los certificados generados a partir de la CSR dentro del producto y para los certificados generados mediante herramientas externas.

- La clave privada de la entrada se valida contra el certificado de host en la entrada.
- El nombre común (CN) del certificado de host se comprueba con el FQDN del host.
- El nombre común (CN) del certificado de host no debe estar vacío ni en blanco y no debe establecerse en localhost.
- La fecha de inicio de la validez no debe ser posterior y la fecha de caducidad del certificado no debe ser pasada.
- Si existe CA intermedia o CA, la fecha de inicio de validez del certificado no debe ser futura y la fecha de caducidad de validez no debe ser pasada.

La clave privada de la entrada no debe estar cifrada. Si hay claves privadas cifradas, el sistema las rechaza.

Ejemplo 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Ejemplo 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Ejemplo 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Descripciones de página para la gestión de certificados

Puede usar la página HTTPS Certificate para ver los certificados de seguridad actuales y generar certificados HTTPS nuevos.

Página HTTPS Certificate

En la página HTTPS Certificate, puede ver el certificado de seguridad actual, descargar una solicitud de firma de certificación, generar un certificado HTTPS autofirmado nuevo o instalar un certificado HTTPS nuevo.

Si no generó un certificado HTTPS autofirmado nuevo, el certificado que aparece en esta página es el certificado que se generó durante la instalación.

Botones de comando

Los botones de comando le permiten realizar las siguientes operaciones:

- **Descargar la solicitud de firma de certificado HTTPS**

  Descarga una solicitud de certificación para el certificado HTTPS instalado actualmente. El explorador le solicita que guarde el archivo <hostname>.csr para poder proporcionar el archivo a una entidad de certificación que desea firmar.

- **Instalar certificado HTTPS**

  Permite cargar e instalar un certificado de seguridad después de que una entidad de certificación lo haya firmado y devuelto. El nuevo certificado se aplicará después de reiniciar el servidor de gestión.

- **Regenerar certificado HTTPS**

  Permite generar un certificado HTTPS autofirmado nuevo, que reemplaza el certificado de seguridad actual. El nuevo certificado se aplica después de reiniciar Unified Manager.

Cuadro de diálogo Regenerate HTTPS Certificate

El cuadro de diálogo Regenerate HTTPS Certificate permite personalizar la información de seguridad y, a continuación, generar un nuevo certificado HTTPS con esa información.

La información del certificado actual aparece en esta página.

La selección "'Regenerate usando atributos de certificado actuales'" y "'Actualizar atributos de certificado actuales'" le permite regenerar el certificado con la información actual o generar un certificado con nueva información.

- **Nombre común**

  Obligatorio. El nombre de dominio completo (FQDN) que desea proteger.

  En las configuraciones de alta disponibilidad de Unified Manager, utilice la dirección IP virtual.

- **Correo electrónico**

  Opcional. Una dirección de correo electrónico para ponerse en contacto con su empresa; normalmente, la dirección de correo electrónico del administrador del certificado o del departamento DE TI.

- **Empresa**

  Opcional. Normalmente el nombre incorporado de su empresa.

- **Departamento**

  Opcional. El nombre del departamento de su empresa.

- * Ciudad*

  Opcional. Ubicación de la ciudad de su empresa.

- **Estado**

  Opcional. La ubicación del estado o provincia, no abreviada, de la compañía.

- **País**

  Opcional. Ubicación del país de su empresa. Este es típicamente un código ISO de dos letras del país.

- **Nombres alternativos**

  Obligatorio. Nombres de dominio adicionales no primarios que se pueden utilizar para tener acceso a este servidor además del host local u otras direcciones de red existentes. Cada nombre alternativo debe separarse con comas.

  Seleccione la casilla de verificación "'excluir información de identificación local (p. ej., localhost)'" si desea eliminar la información de identificación local del campo nombres alternativos del certificado. Cuando se selecciona esta casilla de verificación, sólo se utiliza el campo nombres alternativos lo que se introduce en el campo. Cuando se deja en blanco, el certificado resultante no tendrá ningún campo nombres alternativos.

- **TAMAÑO DE CLAVE (ALGORITMO DE CLAVE: RSA)**

  El algoritmo de clave está establecido en RSA. Puede seleccionar uno de los tamaños de clave: 2048, 3072 ó 4096 bits. El tamaño de clave predeterminado es de 2048 bits.

- **PERÍODO DE VALIDEZ**

  El período de validez predeterminado es de 397 días. Si ha actualizado desde una versión anterior, es posible que la validez del certificado anterior no cambie.

Para obtener más información, consulte "Generación de certificados HTTPS".