Gestión de certificados de seguridad

OnCommand Unified Manager 9.5

NetApp
April 02, 2025

This PDF was generated from https://docs.netapp.com/es-es/oncommand-unified-manager-95/online-help/task-viewing-the-https-security-certificate-ocf.html on April 02, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestión de certificados de seguridad . . . 1
- Visualizar el certificado de seguridad HTTPS . . . 1
  - Antes de empezar . . . 1
  - Acerca de esta tarea . . . 1
  - Pasos . . . 1
  - Después de terminar . . . 1
- Generar un certificado de seguridad HTTPS . . . 1
  - Antes de empezar . . . 1
  - Acerca de esta tarea . . . 1
  - Pasos . . . 2
  - Después de terminar . . . 3
  - Reiniciar la máquina virtual de Unified Manager . . . 3
- Descargar una solicitud de firma de certificación HTTPS . . . 3
  - Antes de empezar . . . 3
  - Pasos . . . 3
  - Después de terminar . . . 3
- Instalar un certificado de seguridad HTTPS . . . 4
  - Antes de empezar . . . 4
  - Pasos . . . 4
  - Ejemplo de cadena de certificados . . . 4
- Descripciones de página para la gestión de certificados . . . 5
  - Página HTTPS Certificate . . . 5
  - Cuadro de diálogo Regenerate HTTPS Certificate . . . 5

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.

Antes de empezar

Debe tener el rol de operador, administrador de OnCommand o administrador del almacenamiento.

Acerca de esta tarea

La visualización del certificado permite verificar el contenido de un certificado regenerado o ver nombres de URL alternativos desde los que puede acceder a Unified Manager.

Pasos

1. En la barra de herramientas, haga clic en Y a continuación, haga clic en **Certificado HTTPS** en el menú **Configuración**.

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

Después de terminar

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.

Generar un certificado de seguridad HTTPS

Puede generar un nuevo certificado de seguridad HTTPS por varios motivos, como si desea firmar con otra entidad emisora de certificados o si el certificado de seguridad actual ha caducado. El nuevo certificado sustituye al certificado existente.

Antes de empezar

Debe tener el rol de administrador de OnCommand.

Acerca de esta tarea

Si no tiene acceso a la interfaz de usuario web de Unified Manager, puede volver a generar el certificado HTTPS con los mismos valores mediante la consola de mantenimiento.

Pasos

1. En la barra de herramientas, haga clic en Y a continuación, haga clic en **Certificado HTTPS** en el menú **Configuración**.
2. Haga clic en **regenerar certificado HTTPS**.

   Aparece el cuadro de diálogo Regenerate HTTPS Certificate.

3. Seleccione una de las siguientes opciones en función de cómo desee generar el certificado:

Si desea…	Realice lo siguiente…
Regenere el certificado con los valores actuales	Haga clic en la opción **Regenerate usando atributos de certificado actuales**.
Genere el certificado con diferentes valores	`Click the *Update the Current Certificate Attributes* option. Los campos Nombre común y nombres alternativos utilizarán los valores del certificado existente si no introduce nuevos valores. Los demás campos no requieren valores, pero puede introducir valores, por ejemplo, para la ciudad, el estado y el país si desea que dichos valores se rellenen en el certificado.` Puede seleccionar 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.

4. Haga clic en **Sí** para regenerar el certificado.
5. Reinicie el servidor de Unified Manager para que el nuevo certificado surta efecto.

Después de terminar

Compruebe la información del nuevo certificado; para ello, consulte el certificado HTTPS.

Reiniciar la máquina virtual de Unified Manager

Puede reiniciar el equipo virtual desde la consola de mantenimiento de Unified Manager. Debe reiniciar después de generar un nuevo certificado de seguridad o si hay un problema con la máquina virtual.

Antes de empezar

El dispositivo virtual está encendido.

Ha iniciado sesión en la consola de mantenimiento como usuario de mantenimiento.

Acerca de esta tarea

También puede reiniciar la máquina virtual desde vSphere mediante la opción **Restart Guest**. Para obtener más información, consulte la documentación de VMware.

Pasos

1. Acceda a la consola de mantenimiento.
2. Seleccione **Configuración del sistema** > **Reiniciar Virtual Machine**.

Descargar una solicitud de firma de certificación HTTPS

Puede descargar una solicitud de certificación para el certificado de seguridad HTTPS actual para poder proporcionar el archivo a una entidad emisora de certificados para firmarlo. 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.

Antes de empezar

Debe tener el rol de administrador de OnCommand.

Pasos

1. En la barra de herramientas, haga clic en Y a continuación, haga clic en **Certificado HTTPS** en el menú **Configuración**.
2. Haga clic en **Descargar la solicitud de firma de certificado HTTPS**.
3. Guarde la `<hostname>.csr` archivo.

Después de terminar

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

Instalar un certificado de seguridad 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.

Antes de empezar

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 el rol de administrador de OnCommand.

Pasos

1. En la barra de herramientas, haga clic en Y a continuación, haga clic en **Certificado HTTPS** en el menú **Configuración**.
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.

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-----
```

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 nuevo o instalar un certificado HTTPS nuevo.

Si no generó un certificado HTTPS 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 navegador le solicitará que guarde la `<hostname>.csr` Para que pueda proporcionar el archivo a una autoridad de certificación para 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, que reemplaza al 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.

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.