Compruebe la identidad de los servidores remotos mediante certificados

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/system-admin/verify-identity-remote-servers-certificates-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Compruebe la identidad de los servidores remotos mediante certificados 1
Compruebe la identidad de los servidores remotos mediante la introducción de certificados 1
Verifique que los certificados digitales sean válidos mediante OCSP 1
Ver certificados predeterminados para aplicaciones basadas en TLS 3

Compruebe la identidad de los servidores remotos mediante certificados

Compruebe la identidad de los servidores remotos mediante la introducción de certificados

ONTAP admite características de certificado de seguridad para verificar la identidad de los servidores remotos.

El software ONTAP permite conexiones seguras utilizando las siguientes funciones y protocolos de certificados digitales:

- El protocolo de estado de certificados en línea (OCSP) valida el estado de las solicitudes de certificados digitales de los servicios de ONTAP mediante conexiones SSL y de seguridad de la capa de transporte (TLS). Esta función está deshabilitada de forma predeterminada.
- Con el software ONTAP se incluye un conjunto predeterminado de certificados raíz de confianza.
- Los certificados de protocolo de interoperabilidad de gestión de claves (KMIP) permiten la autenticación mutua de un clúster y de un servidor KMIP.

Verifique que los certificados digitales sean válidos mediante OCSP

A partir de ONTAP 9.2, el protocolo de estado de certificado en línea (OCSP) habilita las aplicaciones ONTAP que utilizan comunicaciones de seguridad de capa de transporte (TLS) para recibir el estado de certificado digital cuando OCSP está habilitado. Es posible habilitar o deshabilitar las comprobaciones de estado de certificados de OCSP para aplicaciones específicas en cualquier momento. De manera predeterminada, la comprobación del estado de los certificados OCSP está deshabilitada.

Lo que necesitará

Necesita acceso de nivel de privilegio avanzado para realizar esta tarea.

Acerca de esta tarea

OCSP admite las siguientes aplicaciones:

- AutoSupport
- Sistema de gestión de eventos (EMS)
- LDAP sobre TLS
- Protocolo de interoperabilidad de gestión de claves (KMIP)
- Registro de auditoría
- FabricPool
- SSH (a partir de ONTAP 9.13.1)

Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`.
2. Para habilitar o deshabilitar las comprobaciones de estado de certificados de OCSP para aplicaciones de ONTAP específicas, utilice el comando correspondiente.

Si desea que las comprobaciones del estado del certificado OCSP para que algunas aplicaciones sean…	Usar el comando…
Activado	`security config ocsp enable -app` app name
Deshabilitado	`security config ocsp disable -app` app name

El siguiente comando habilita la compatibilidad de OCSP para AutoSupport y EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

Cuando OCSP está habilitado, la aplicación recibe una de las siguientes respuestas:

- Correcto: El certificado es válido y la comunicación continúa.
- Revocado: La autoridad emisora de certificados considera permanentemente que el certificado no es de confianza y la comunicación no continúa.
- Unknown: El servidor no tiene ninguna información de estado sobre el certificado y la comunicación no continúa.
- Falta información del servidor OCSP en el certificado: El servidor actúa como si OCSP está deshabilitado y continúa con la comunicación TLS, pero no se produce ninguna comprobación de estado.
- Sin respuesta del servidor OCSP: La aplicación no puede continuar.

3. Para habilitar o deshabilitar las comprobaciones de estado de certificados OCSP para todas las aplicaciones que utilizan comunicaciones TLS, utilice el comando correspondiente.

Si desea que las comprobaciones del estado del certificado OCSP para que todas las aplicaciones sean…	Usar el comando…

Activado	`security config ocsp enable`
	
	`-app all`

Deshabilitado	`security config ocsp disable`
	
	`-app all`

Cuando se habilita, todas las aplicaciones reciben una respuesta firmada que significa que el certificado especificado es correcto, revocado o desconocido. En el caso de un certificado revocado, la solicitud no

continuará. Si la aplicación no recibe una respuesta del servidor OCSP o si no se puede acceder al servidor, la aplicación no podrá continuar.

4. Utilice la `security config ocsp show` Comando para mostrar todas las aplicaciones compatibles con OCSP y su estado de soporte.

```
cluster::*> security config ocsp show
         Application                        OCSP Enabled?
         --------------------               ---------------------
         autosupport                        false
         audit_log                          false
         fabricpool                         false
         ems                                false
         kmip                               false
         ldap_ad                            true
         ldap_nis_namemap                   true
         ssh                                true

         8 entries were displayed.
```

Ver certificados predeterminados para aplicaciones basadas en TLS

A partir de ONTAP 9.2, ONTAP proporciona un conjunto predeterminado de certificados raíz de confianza para aplicaciones ONTAP que utilizan Seguridad de la capa de transporte (TLS).

Lo que necesitará

Los certificados predeterminados solo se instalan en la SVM de administrador durante su creación o durante una actualización a ONTAP 9.2.

Acerca de esta tarea

Las aplicaciones actuales que funcionan como cliente y requieren validación de certificados son AutoSupport, EMS, LDAP, Registro de auditoría, FabricPool, Y KMIP.

Cuando los certificados caducan, se invoca un mensaje EMS que solicita al usuario que elimine los certificados. Los certificados predeterminados solo se pueden eliminar en el nivel de privilegios avanzados.

> La eliminación de los certificados predeterminados puede provocar que algunas aplicaciones ONTAP no funcionen como se esperaba (por ejemplo, AutoSupport y Registro de auditoría).

Paso

1. Puede ver los certificados predeterminados que se instalan en la SVM de administrador mediante el comando Security certificate show:

   `security certificate show -vserver –type server-ca`

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver    Serial Number   Common Name                             Type
---------- --------------- ---------------------------------------
------------
fas2552-2n-abc-3
           01              AAACertificateServices
server-ca
    Certificate Authority: AAA Certificate Services
          Expiration Date: Sun Dec 31 18:59:59 2028
```

Información de copyright

Copyright © 2024 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.