Uso de Kerberos con NFS para una mayor seguridad

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Uso de Kerberos con NFS para una mayor seguridad

Compatibilidad de ONTAP NFS con Kerberos

Kerberos proporciona una autenticación segura y segura para aplicaciones cliente/servidor. La autenticación permite verificar las identidades de usuario y proceso a un servidor. En el entorno de ONTAP, Kerberos proporciona autenticación entre máquinas virtuales de almacenamiento (SVM) y clientes NFS.

En ONTAP 9, se admiten las siguientes funcionalidades de Kerberos:

- Autenticación Kerberos 5 con comprobación de integridad (krb5i)

  Krb5i utiliza sumas de comprobación para verificar la integridad de cada mensaje de NFS transferido entre el cliente y el servidor. Esto resulta útil por motivos de seguridad (por ejemplo, para garantizar que los datos no se han alterado) y por motivos de integridad de los datos (por ejemplo, para evitar que se dañen los datos cuando se utilizan NFS en redes no fiables).

- Autenticación Kerberos 5 con comprobación de privacidad (krb5p)

  Krb5p utiliza sumas de comprobación para cifrar todo el tráfico entre cliente y servidor. Esto es más seguro y también implica más carga.

- Cifrado AES de 128 bits y 256 bits

  El estándar de cifrado avanzado (AES) es un algoritmo de cifrado para proteger los datos electrónicos. ONTAP admite AES con claves de 128 bits (AES-128) y AES con cifrado de claves de 256 bits (AES-256) para Kerberos para mayor seguridad.

- Configuraciones en dominio de Kerberos a nivel de SVM

  Los administradores de SVM ahora pueden crear configuraciones de dominio de Kerberos en el nivel de SVM. Esto significa que los administradores de SVM ya no tienen que depender del administrador de clúster para la configuración de dominio de Kerberos y pueden crear configuraciones de dominio de Kerberos individuales en un entorno multi-tenancy.

Requisitos para configurar Kerberos con ONTAP NFS

Antes de configurar Kerberos con NFS en el sistema, debe comprobar que determinados elementos de la red y el entorno de almacenamiento están configurados correctamente.

Los pasos para configurar su entorno dependen de qué versión y tipo del sistema operativo cliente, controlador de dominio, Kerberos, DNS, etc., que usted está usando. La documentación de todas estas variables está fuera del alcance de este documento. Para obtener más información, consulte la documentación correspondiente de cada componente.

Para obtener un ejemplo detallado de cómo configurar ONTAP y Kerberos 5 con NFSv3 y NFSv4 en un entorno mediante hosts de Windows Server 2008 R2 Active Directory y Linux, consulte el informe técnico 4073.

Primero deben configurarse los siguientes elementos:

Requisitos del entorno de red

- Kerberos

  Debe tener una configuración Kerberos en funcionamiento con un centro de distribución de claves (KDC), como Kerberos basado en Windows Active Directory o MIT Kerberos.

  Los servidores NFS deben `nfs` utilizar como componente principal de su principal máquina.

- Servicio de directorio

  Debe utilizar un servicio de directorio seguro en su entorno, como Active Directory u OpenLDAP, que esté configurado para usar LDAP sobre SSL/TLS.

- NTP

  Debe tener un servidor de tiempo de trabajo que ejecute NTP. Esto es necesario para evitar errores de autenticación de Kerberos debido a una desviación de tiempo.

- Resolución de nombres de dominio (DNS)

  Cada cliente UNIX y cada LIF de SVM deben tener un registro de servicio (SRV) adecuado registrado con el KDC en zonas de búsqueda inversa y de reenvío. Todos los participantes deben poder resolverse correctamente a través de DNS.

- Cuentas de usuario

  Cada cliente debe tener una cuenta de usuario en el dominio Kerberos. Los servidores NFS deberán utilizar «'nfs» como componente principal de su principal equipo.

Requisitos del cliente NFS

- NFS

  Cada cliente debe estar configurado correctamente para comunicarse a través de la red mediante NFSv3 o NFSv4.

  Los clientes deben admitir RFC1964 y RFC2203.

- Kerberos

  Cada cliente debe estar configurado correctamente para utilizar la autenticación Kerberos, incluidos los siguientes detalles:

  - El cifrado para la comunicación TGS está activado.

    AES-256 para obtener la máxima seguridad.

  - El tipo de cifrado más seguro para la comunicación TGT está activado.
  - El dominio y el dominio de Kerberos están configurados correctamente.
  - GSS está activado.

Al utilizar las credenciales de la máquina:

  - No se debe ejecutar `gssd` con el `-n` parámetro.
  - No ejecute `kinit` como usuario root.

- Cada cliente debe utilizar la versión más reciente y actualizada del sistema operativo.

  Esto proporciona la mejor compatibilidad y fiabilidad para el cifrado AES con Kerberos.

- DNS

  Cada cliente debe estar configurado correctamente para utilizar DNS con la resolución de nombres correcta.

- NTP

  Cada cliente debe sincronizarse con el servidor NTP.

- Información sobre el host y el dominio

  ```
  `/etc/hosts` `/etc/resolv.conf`Los archivos y de cada cliente deben
  contener el nombre de host e información de DNS correctos,
  respectivamente.
  ```

- Archivos keytab

  Cada cliente debe tener un archivo keytab del KDC. El Reino debe estar en letras mayúsculas. El tipo de cifrado debe ser AES-256 para obtener una seguridad más potente.

- Opcional: Para obtener el mejor rendimiento, los clientes se benefician de tener al menos dos interfaces de red: Una para comunicarse con la red de área local y otra para comunicarse con la red de almacenamiento.

Requisitos del sistema de almacenamiento

- Licencia de NFS

  El sistema de almacenamiento debe tener instalada una licencia NFS válida.

- Licencia CIFS

  La licencia CIFS es opcional. Sólo es necesario comprobar las credenciales de Windows cuando se utiliza la asignación de nombres multiprotocolo. No es necesario en entornos estrictos sólo UNIX.

- SVM

  Debe tener al menos una SVM configurada en el sistema.

- DNS en la SVM

  Debe haber configurado DNS en cada SVM.

- Servidor NFS

Debe haber configurado NFS en la SVM.

- Cifrado AES

  Para obtener la mayor seguridad, debe configurar el servidor NFS para permitir solo el cifrado AES-256 para Kerberos.

- Servidor SMB

  Si ejecuta un entorno multiprotocolo, debe haber configurado SMB en la SVM. Se requiere el servidor SMB para la asignación de nombres multiprotocolo.

- Volúmenes

  Debe tener un volumen raíz y, al menos, un volumen de datos configurado para que lo utilice la SVM.

- Volumen raíz

  El volumen raíz de la SVM debe tener la siguiente configuración:

Nombre	Ajuste
Estilo de seguridad	UNIX
UID	Raíz o ID 0
GID	Raíz o ID 0
Permisos de UNIX	777

  A diferencia del volumen raíz, los volúmenes de datos pueden tener cualquier estilo de seguridad.

- Grupos UNIX

  La SVM debe tener configurados los siguientes grupos UNIX:

Nombre del grupo	ID de grupo
daemon	1
raíz	0
pcuser	65534 (creado automáticamente por ONTAP cuando se crea la SVM)

- Usuarios de UNIX

  La SVM debe tener configurados los siguientes usuarios de UNIX:

Nombre de usuario	ID de usuario	ID del grupo principal	Comentar
nfs	500	0	Necesario para la fase de INICIO DE GSS El primer componente del SPN de usuario del cliente NFS se utiliza como usuario.
pcuser	65534	65534	Necesario para el uso multiprotocolo de NFS y CIFS ONTAP lo crea y añade automáticamente al grupo pcuser cuando crea la SVM.
raíz	0	0	Necesario para el montaje

El usuario nfs no es necesario si existe una asignación de nombre Kerberos-UNIX para el SPN del usuario cliente NFS.

- Reglas y políticas de exportación

  Debe haber configurado políticas de exportación con las reglas de exportación necesarias para los volúmenes raíz y de datos y qtrees. Si se accede a todos los volúmenes de SVM mediante Kerberos, puede establecer las opciones de la regla de exportación `-rorule` , `-rwrule` y `-superuser` para el volumen raíz en `krb5` , `krb5i` o `krb5p`.

- Asignación de nombres Kerberos-UNIX

  Si desea que el usuario identificado por el SPN de usuario del cliente NFS tenga permisos raíz, debe crear una asignación de nombre a root.

Información relacionada

"Informe técnico de NetApp 4073: Autenticación unificada segura"

"Herramienta de matriz de interoperabilidad de NetApp"

"Administración del sistema"

"Gestión de almacenamiento lógico"

Especifique el dominio de ID de usuario de ONTAP para NFSv4

Para especificar el dominio de ID de usuario, puede establecer la `-v4-id-domain` opción.

Acerca de esta tarea

De forma predeterminada, ONTAP utiliza el dominio NIS para la asignación del ID de usuario de NFSv4, si hay algún establecido. Si no se establece un dominio NIS, se utiliza el dominio DNS. Es posible que deba establecer el dominio de ID de usuario si, por ejemplo, tiene varios dominios de ID de usuario. El nombre de dominio debe coincidir con la configuración de dominio del controlador de dominio. No es necesaria para NFSv3.

Paso

1. Introduzca el siguiente comando:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Información de copyright

Información de la marca comercial