Utilice Kerberos con NFS para una mayor seguridad

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Utilice Kerberos con NFS para una mayor seguridad

Información general sobre cómo utilizar Kerberos con NFS para una mayor seguridad

Si se utiliza Kerberos en su entorno para autenticación segura, debe trabajar con el administrador de Kerberos para determinar requisitos y configuraciones del sistema de almacenamiento apropiadas y, a continuación, habilitar la SVM como cliente Kerberos.

Su entorno debe cumplir las siguientes directrices:

- La implementación de su sitio debe seguir las prácticas recomendadas para la configuración del servidor Kerberos y del cliente antes de configurar Kerberos para ONTAP.
- Si es posible, utilice NFSv4 o posteriores si es necesaria la autenticación de Kerberos.

  NFSv3 se puede utilizar con Kerberos. Sin embargo, todas las ventajas de seguridad de Kerberos solo se materian en puestas en marcha de ONTAP de NFSv4 o posteriores.

- Para promover el acceso redundante al servidor, se debe habilitar Kerberos en varias LIF de datos en varios nodos del clúster mediante el mismo SPN.
- Cuando se habilita Kerberos en la SVM, debe especificarse uno de los siguientes métodos de seguridad en las reglas de exportación para volúmenes o qtrees en función de la configuración del cliente NFS.
  - `krb5` (Protocolo Kerberos v5)
  - `krb5i` (Protocolo Kerberos v5 con comprobación de integridad con sumas de comprobación)
  - `krb5p` (Protocolo Kerberos v5 con servicio de privacidad)

Además del servidor Kerberos y los clientes, para ONTAP se deben configurar los siguientes servicios externos con el fin de admitir Kerberos:

- 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. No utilice NIS, cuyas solicitudes se envían en texto claro y, por lo tanto, no son seguras.

- 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.

Verifique los permisos para la configuración de Kerberos

Kerberos requiere que se establezcan determinados permisos de UNIX para el volumen raíz de la SVM y para los usuarios y grupos locales.

Pasos

1. Visualice los permisos relevantes en el volumen raíz de la SVM:

   `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`

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

Nombre…	Estableciendo…
UID	Raíz o ID 0
GID	Raíz o ID 0
Permisos UNIX	755

   Si no se muestran estos valores, utilice `volume modify` comando para actualizarlos.

2. Mostrar los usuarios UNIX locales:

   `vserver services name-service unix-user show -vserver` *`vserver_name`*

   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 INICIALIZACIÓN de GSS. El primer componente del SPN de usuario del cliente NFS se utiliza como usuario. El usuario nfs no es necesario si existe una asignación de nombre Kerberos-UNIX para el SPN del usuario cliente NFS.
raíz	0	0	Necesario para el montaje.

   Si no se muestran estos valores, puede usar `vserver services name-service unix-user`

`modify` comando para actualizarlos.

3. Mostrar los grupos UNIX locales:

   `vserver services name-service unix-group show -vserver vserver _name`

   La SVM debe tener configurados los siguientes grupos UNIX:

Nombre del grupo	ID de grupo
daemon	1
raíz	0

   Si no se muestran estos valores, puede usar `vserver services name-service unix-group modify` comando para actualizarlos.

Cree una configuración de dominio de Kerberos para NFS

Si desea que ONTAP acceda a servidores Kerberos externos en su entorno, primero debe configurar la SVM para que utilice un Reino de Kerberos existente. Para ello, necesita recopilar valores de configuración para el servidor Kerberos KDC y, a continuación, utilizar `vserver nfs kerberos realm create` Comando para crear la configuración de dominio de Kerberos en una SVM.

Lo que necesitará

El administrador del clúster debe haber configurado NTP en el sistema de almacenamiento, el cliente y el servidor KDC para evitar problemas de autenticación. Las diferencias de tiempo entre un cliente y un servidor (desfase de reloj) son una causa común de fallos de autenticación.

Pasos

1. Consulte con su administrador Kerberos para determinar los valores de configuración adecuados para suministrar con `vserver nfs kerberos realm create` comando.
2. Cree una configuración de dominio de Kerberos en la SVM:

   `vserver nfs kerberos realm create -vserver vserver_name -realm realm_name {AD_KDC_server_values |AD_KDC_server_values} -comment "text"`

3. Compruebe que la configuración de dominio Kerberos se ha creado correctamente:

   `vserver nfs kerberos realm show`

Ejemplos

El siguiente comando crea una configuración de dominio Kerberos para NFS para la SVM vs1 que utiliza un servidor de Microsoft Active Directory como servidor KDC. El dominio Kerberos es AUTH.EXAMPLE.COM. El servidor de Active Directory se denomina ad-1 y su dirección IP es 10.10.8.14. La desviación del reloj permitida es de 300 segundos (valor predeterminado). La dirección IP del servidor KDC es 10.10.8.14 y su número de puerto es 88 (el valor predeterminado). "Microsoft Kerberos config" es el comentario.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

El siguiente comando crea una configuración de dominio de Kerberos para NFS para la SVM vs1 que utiliza un MIT KDC. El dominio Kerberos es SECURITY.EXAMPLE.COM. La desviación del reloj permitida es de 300 segundos. La dirección IP del servidor KDC es 10.10.9.1 y su número de puerto es 88. El proveedor de KDC es otro que indica un proveedor de UNIX. La dirección IP del servidor de administración es 10.10.9.1 y su número de puerto es 749 (el valor predeterminado). La dirección IP del servidor de contraseñas es 10.10.9.1 y su número de puerto es 464 (el valor predeterminado). "UNIX Kerberos config" es el comentario.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configurar los tipos de cifrado permitidos de Kerberos para NFS

De forma predeterminada, ONTAP admite los siguientes tipos de cifrado para NFS Kerberos: DES, 3DES, AES-128 y AES-256. Puede configurar los tipos de cifrado permitidos para cada SVM para adaptarse a los requisitos de seguridad de su entorno concreto mediante el `vserver nfs modify` con el `-permitted-enc-types` parámetro.

Acerca de esta tarea

Para obtener la mayor compatibilidad del cliente, ONTAP admite de forma predeterminada tanto el cifrado des débil como el AES sólido. Esto significa, por ejemplo, que si desea aumentar la seguridad y su entorno lo admite, puede utilizar este procedimiento para deshabilitar DES y 3DES y requerir que los clientes utilicen sólo el cifrado AES.

Debería utilizar el cifrado más potente disponible. Para ONTAP, esto es AES-256. Debe confirmar con el administrador de KDC que este nivel de cifrado es compatible con su entorno.

- Habilitar o deshabilitar completamente AES (tanto AES-128 como AES-256) en las SVM es disruptivo porque destruye el archivo ORIGINAL DE DES principal/keytab, lo que requiere que se deshabilite la configuración de Kerberos en todos los LIF para la SVM.

  Antes de realizar este cambio, debe comprobar que los clientes NFS no utilizan el cifrado AES en la SVM.

- La habilitación o deshabilitación DE DES o 3DES no requiere ningún cambio en la configuración de Kerberos en las LIF.

Paso

1. Habilite o deshabilite el tipo de cifrado permitido que desee:

Si desea habilitar o deshabilitar…	Siga estos pasos…
DES o 3DES	a. Configure los tipos de cifrado de la SVM permitidos por NFS Kerberos: `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Separe varios tipos de cifrado con una coma. b. Compruebe que el cambio se ha realizado correctamente: `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

AES-128 o AES-256	a. Identificar en qué SVM y Kerberos de LIF están habilitados:
	`vserver nfs kerberos interface show`
	
	b. Deshabilite Kerberos en todas las LIF de la SVM cuyo NFS Kerberos permitió el tipo de cifrado que desea modificar:
	`vserver nfs kerberos interface disable -lif` *`lif_name`*
	
	c. Configure los tipos de cifrado de la SVM permitidos por NFS Kerberos:
	`vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`*
	
	Separe varios tipos de cifrado con una coma.
	
	d. Compruebe que el cambio se ha realizado correctamente:
	`vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`
	
	e. Vuelva a habilitar Kerberos en todas las LIF en la SVM:
	`vserver nfs kerberos interface enable -lif` *`lif_name`* `-spn` *`service_principal_name`*
	
	f. Compruebe que Kerberos está habilitado en todas las LIF:
	`vserver nfs kerberos interface show`

Habilite Kerberos en una LIF de datos

Puede utilizar el `vserver nfs kerberos interface enable` Comando para habilitar Kerberos en una LIF de datos. Esto permite que la SVM utilice servicios de seguridad Kerberos para NFS.

Acerca de esta tarea

Si utiliza un KDC de Active Directory, los primeros 15 caracteres de los SPN utilizados deben ser únicos entre las SVM dentro de un dominio o dominio.

Pasos

1. Cree la configuración de Kerberos NFS:

   `vserver nfs kerberos interface enable -vserver` *`vserver_name`* `-lif` *`logical_interface`* `-spn` *`service_principal_name`*

   ONTAP requiere la clave secreta del SPN desde el KDC para habilitar la interfaz Kerberos.

   Para los KDC de Microsoft, se contacta con el KDC y se emite un mensaje de nombre de usuario y contraseña en la CLI para obtener la clave secreta. Si necesita crear el SPN en una unidad organizativa diferente del dominio Kerberos, puede especificar el opcional `-ou` parámetro.

   Para los KDC que no son de Microsoft, la clave secreta se puede obtener utilizando uno de los dos métodos:

Si…	También debe incluir el siguiente parámetro con el comando…
Tenga las credenciales de administrador de KDC para recuperar la clave directamente desde el KDC	`-admin-username` *`kdc_admin_username`*
No tiene las credenciales de administrador de KDC, pero tiene un archivo keytab del KDC que contiene la clave	`-keytab-uri` {ftp

2. Compruebe que Kerberos estaba habilitado en la LIF:

   `vserver nfs kerberos-config show`

3. Repita los pasos 1 y 2 para habilitar Kerberos en varios LIF.

Ejemplo

El siguiente comando crea y verifica una configuración Kerberos de NFS para la SVM denominada vs1 en la interfaz lógica ves03-d1, con el SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM en la OU lab2ou:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- -------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```