Verifique el acceso mediante el seguimiento de seguridad

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Verifique el acceso mediante el seguimiento de seguridad

Cómo funcionan los seguimientos de seguridad

Puede añadir filtros de seguimiento de permisos para indicarle a ONTAP que registre la información sobre por qué los servidores SMB y NFS de una máquina virtual de almacenamiento (SVM) permiten o deniega la solicitud de un cliente o usuario para realizar una operación. Esto puede ser útil si desea verificar que el esquema de seguridad de acceso a archivos es adecuado o si desea solucionar problemas de acceso a archivos.

Los seguimientos de seguridad permiten configurar un filtro que detecta las operaciones del cliente en SMB y NFS en la SVM, y realizar el seguimiento de todas las comprobaciones de acceso que coinciden con ese filtro. A continuación, puede ver los resultados de la traza, lo que proporciona un resumen práctico de la razón por la que se permitió o denegó el acceso.

Cuando desee verificar la configuración de seguridad para el acceso SMB o NFS en los archivos y carpetas de la SVM o si tiene algún problema de acceso, puede añadir rápidamente un filtro para activar el seguimiento de permisos.

En la siguiente lista, se describen aspectos importantes sobre el funcionamiento de los seguimientos de seguridad:

- ONTAP aplica seguimientos de seguridad a nivel de SVM.
- Cada solicitud entrante se realiza un análisis para ver si coincide con los criterios de filtrado de cualquier seguimiento de seguridad activado.
- Los seguimientos se realizan tanto para solicitudes de acceso a archivos como a carpetas.
- Los seguimientos pueden filtrarse según los criterios siguientes:
  - IP del cliente
  - Ruta SMB o NFS
  - Nombre de Windows
  - Nombre UNIX
- Las solicitudes se someten a un análisis de los resultados de respuesta de acceso *Allowed* y *denied*.
- Cada solicitud que coincide con los criterios de filtrado de trazas activadas se registra en el registro de resultados de seguimiento.
- El administrador de almacenamiento puede configurar un tiempo de espera en un filtro para deshabilitarlo automáticamente.
- Si una solicitud coincide con varios filtros, se registran los resultados del filtro con el número de índice más alto.
- El administrador de almacenamiento puede imprimir los resultados del registro de resultados de rastreo para determinar por qué se permitió o denegó una solicitud de acceso.

Tipos de acceso comprueba el monitor de seguimiento de seguridad

Las comprobaciones de acceso de un archivo o una carpeta se realizan según varios criterios. Los seguimientos de seguridad supervisan las operaciones con todos estos criterios.

Los tipos de comprobaciones de acceso que supervisa el seguimiento de seguridad incluyen los siguientes:

- Estilo de seguridad del volumen y del qtree
- Seguridad efectiva del sistema de archivos que contiene los archivos y carpetas en los que se solicitan operaciones
- Asignación de usuarios
- Permisos a nivel de recurso compartido
- Permisos a nivel de exportación
- Permisos a nivel de archivo
- Seguridad para proteger el acceso al nivel de almacenamiento

Consideraciones que tener en cuenta al crear seguimientos de seguridad

Debe tener en cuenta diferentes consideraciones cuando cree seguimientos de seguridad en máquinas virtuales de almacenamiento (SVM). Por ejemplo, debe saber en qué protocolos puede crear una traza, qué estilos de seguridad son compatibles y cuál es el número máximo de trazas activas.

- Solo puede crear seguimientos de seguridad en las SVM.
- Cada entrada del filtro de seguimiento de seguridad es específica para la SVM.

  Debe especificar la SVM donde desee ejecutar el seguimiento.

- Puede agregar filtros de seguimiento de permisos para solicitudes SMB y NFS.
- Debe configurar el servidor SMB o NFS en la SVM donde desee crear filtros de seguimiento.
- Puede crear seguimientos de seguridad para archivos y carpetas que residen en volúmenes y qtrees de estilo de seguridad NTFS, UNIX y mixtos.
- Puede añadir un máximo de 10 filtros de seguimiento de permisos por SVM.
- Debe especificar un número de índice de filtro al crear o modificar un filtro.

  Los filtros se tienen en cuenta por orden del número de índice. Los criterios de un filtro con un número de índice más alto se tienen en cuenta antes que los criterios con un número de índice más bajo. Si la solicitud que se realiza el seguimiento coincide con los criterios de varios filtros habilitados, sólo se activa el filtro con el número de índice más alto.

- Una vez creado y habilitado un filtro de seguimiento de seguridad, debe realizar algunas solicitudes de archivo o carpeta en un sistema cliente para generar la actividad que el filtro de seguimiento pueda capturar e iniciar sesión en el registro de resultados de seguimiento.

- Debe agregar filtros de seguimiento de permisos sólo para fines de verificación de acceso a archivos o solución de problemas.

  La adición de filtros de seguimiento de permisos tiene un efecto secundario en el rendimiento de la controladora.

  Cuando haya terminado con la actividad de verificación o solución de problemas, deberá desactivar o quitar todos los filtros de seguimiento de permisos. Además, los criterios de filtrado que seleccione deben ser lo más específicos posible para que ONTAP no envíe un gran número de resultados de seguimiento al registro.

Realizar seguimientos de seguridad

Realice información general sobre los seguimientos de seguridad

La realización de un seguimiento de seguridad implica la creación de un filtro de seguimiento de seguridad, la verificación de los criterios de filtro, la generación de solicitudes de acceso en un cliente SMB o NFS que coincida con los criterios de filtro y la visualización de los resultados.

Una vez que haya terminado de utilizar un filtro de seguridad para capturar información de seguimiento, puede modificar el filtro y reutilizarlo, o bien deshabilitarlo si ya no lo necesita. Después de ver y analizar los resultados de la traza del filtro, puede eliminarlos si ya no son necesarios.

Cree filtros de seguimiento de seguridad

Es posible crear filtros de seguimiento de seguridad que detecten operaciones de cliente SMB y NFS en máquinas virtuales de almacenamiento (SVM) y realizar un seguimiento de todas las comprobaciones de acceso que coincidan con el filtro. Puede utilizar los resultados de los seguimientos de seguridad para validar la configuración o solucionar problemas de acceso.

Acerca de esta tarea

Hay dos parámetros necesarios para el comando vserver Security trace filter create:

Parámetros necesarios	Descripción
`-vserver vserver_name`	*SVM name* El nombre de la SVM que contiene los archivos o las carpetas en los que se desea aplicar el filtro de seguimiento de seguridad.
`-index index_number`	*Número de índice de filtro* El número de índice que desea aplicar al filtro. Está limitado a un máximo de 10 filtros de seguimiento por SVM. Los valores permitidos para este parámetro son de 1 a 10.

Varios parámetros de filtro opcionales le permiten personalizar el filtro de seguimiento de seguridad para limitar los resultados generados por el seguimiento de seguridad:

Parámetro de filtro	Descripción
`-client-ip` `IP_Address`	Este filtro especifica la dirección IP desde la cual el usuario accede a la SVM.
`-path` `path`	Este filtro especifica la ruta en la que se aplicará el filtro de seguimiento de permisos. Valor para `-path` puede utilizar cualquiera de los siguientes formatos: • La ruta de acceso completa, que comienza desde la raíz del recurso compartido o la exportación • Una ruta parcial, relativa a la raíz del recurso compartido Debe usar los separadores de directorios de estilo UNIX del directorio de estilo NFS en el valor de la ruta.
`-windows-name` `win_user_name` o. `-unix` `-name``unix_user_name`	Puede especificar el nombre de usuario de Windows o el nombre de usuario de UNIX cuyas solicitudes de acceso desea rastrear. La variable de nombre de usuario no distingue mayúsculas y minúsculas. No puede especificar tanto un nombre de usuario de Windows como un nombre de usuario de UNIX en el mismo filtro. Aunque se pueden realizar el seguimiento de eventos de acceso SMB y NFS, es posible que se utilicen el usuario UNIX asignado y los grupos de usuarios UNIX asignados al realizar comprobaciones de acceso a datos de estilo de seguridad mixtos o UNIX.
`-trace-allow` {`yes`	`no`}
El seguimiento de los eventos Denegar siempre está habilitado para un filtro de seguimiento de seguridad. Opcionalmente, es posible realizar el seguimiento de los eventos de permitir. Para realizar el seguimiento de los eventos de permitir, este parámetro se debe establecer en `yes`.	`-enabled` {`enabled`
`disabled`}	Es posible habilitar o deshabilitar el filtro de seguimiento de seguridad. De manera predeterminada, el filtro de seguimiento de seguridad está habilitado.
`-time-enabled` `integer`	Puede especificar un tiempo de espera para el filtro, después del cual se deshabilita.

Pasos

1. Cree un filtro de seguimiento de seguridad:

```
vserver security trace filter create -vserver vserver_name -index
index_numberfilter_parameters
```

`filter_parameters` es una lista de parámetros de filtro opcionales.

Para obtener más información, consulte las páginas de manual del comando.

2. Compruebe la entrada del filtro de seguimiento de seguridad:

```
vserver security trace filter show -vserver vserver_name -index index_number
```

Ejemplos

El siguiente comando crea un filtro de seguimiento de seguridad para cualquier usuario que acceda a un archivo con una ruta de acceso compartida `\\server\share1\dir1\dir2\file.txt` Desde la dirección IP 10.10.10.7. El filtro utiliza una ruta completa para el `-path` opción. La dirección IP del cliente utilizada para acceder a los datos es 10.10.10.7. El filtro se agota el tiempo de espera después de 30 minutos:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
```

El siguiente comando crea un filtro de seguimiento de seguridad mediante una ruta relativa para `-path` opción. El filtro rastrea el acceso de un usuario de Windows llamado "'joe'". Joe está accediendo a un archivo con una ruta de acceso compartido `\\server\share1\dir1\dir2\file.txt`. Los seguimientos de filtro permiten y niegan eventos:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                                Vserver: vs1
                           Filter Index: 2
              Client IP Address to Match: -
                                   Path: /dir1/dir2/file.txt
                     Windows User Name: mydomain\joe
                        UNIX User Name: -
                    Trace Allow Events: yes
                        Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

Muestra información acerca de los filtros de seguimiento de seguridad

Es posible ver información sobre los filtros de seguimiento de seguridad configurados en la máquina virtual de almacenamiento (SVM). Esto le permite ver qué tipos de eventos de acceso tienen cada seguimiento de filtro.

Paso

1. Muestra información acerca de las entradas del filtro de seguimiento de seguridad mediante `vserver security trace filter show` comando.

   Para obtener más información acerca de cómo utilizar este comando, consulte las páginas man.

Ejemplos

El siguiente comando muestra información sobre todos los filtros de seguimiento de seguridad en la SVM vs1:

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

Mostrar resultados de rastreo de seguridad

Puede mostrar los resultados de seguimiento de seguridad generados para las operaciones de archivo que coinciden con los filtros de seguimiento de seguridad. Puede utilizar los resultados para validar la configuración de seguridad del acceso a los archivos o para solucionar problemas de acceso a los archivos SMB y NFS.

Lo que necesitará

Debe existir un filtro de seguimiento de seguridad habilitado y las operaciones deben haberse realizado desde un cliente SMB o NFS que coincida con el filtro de seguimiento de seguridad para generar los resultados de seguimiento de seguridad.

Acerca de esta tarea

Puede mostrar un resumen de todos los resultados de seguimiento de seguridad o puede personalizar la información que se muestra en el resultado especificando parámetros opcionales. Esto puede ser útil cuando los resultados de la traza de seguridad contienen un gran número de registros.

Si no especifica ninguno de los parámetros opcionales, se muestra lo siguiente:

- El nombre de la máquina virtual de almacenamiento (SVM)
- Nombre del nodo
- Número de índice de seguimiento de seguridad
- Estilo de seguridad

- Ruta
- Razón
- Nombre de usuario

  El nombre de usuario se mostrará en función de la configuración del filtro de seguimiento:

Si el filtro está configurado…	Realice lo siguiente…
Con un nombre de usuario UNIX	El resultado de la traza de seguridad muestra el nombre de usuario de UNIX.
Con un nombre de usuario de Windows	El resultado de la traza de seguridad muestra el nombre de usuario de Windows.
Sin un nombre de usuario	El resultado de la traza de seguridad muestra el nombre de usuario de Windows.

Puede personalizar la salida utilizando parámetros opcionales. Algunos de los parámetros opcionales que se pueden utilizar para refinar los resultados devueltos en el resultado del comando son los siguientes:

Parámetro opcional	Descripción
`-fields field_name, ...`	Muestra el resultado en los campos que elija. Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales.
`-instance`	Muestra información detallada acerca de los eventos de seguimiento de seguridad. Use este parámetro con otros parámetros opcionales para mostrar información detallada sobre los resultados específicos del filtro.
`-node node_name`	Muestra información solo sobre eventos en el nodo especificado.
`-vserver vserver_name`	Muestra información solo sobre eventos en la SVM especificada.
`-index integer`	Muestra información sobre los eventos que ocurrieron como resultado del filtro correspondiente al número de índice especificado.
`-client-ip IP_address`	Muestra información sobre los eventos ocurridos como resultado del acceso a archivos desde la dirección IP del cliente especificada.
`-path path`	Muestra información sobre los eventos producidos como resultado del acceso a archivos a la ruta especificada.
`-user-name user_name`	Muestra información acerca de los eventos que ocurrieron como resultado del acceso a archivos por parte del usuario de Windows o UNIX especificado.

`-security-style security_style`	Muestra información sobre los eventos que ocurrieron en sistemas de archivos con el estilo de seguridad especificado.

Consulte la página man para obtener información sobre otros parámetros opcionales que puede utilizar con el comando.

Paso

1. Mostrar los resultados del filtro de seguimiento de seguridad mediante la `vserver security trace trace-result show` comando.

   `vserver security trace trace-result show -user-name domain\user`

   ```
   Vserver: vs1

   Node     Index   Filter Details         Reason
   -------- ------- ---------------------  ----------------------------
   node1    3       User:domain\user       Access denied by explicit ACE
                    Security Style:mixed
                    Path:/dir1/dir2/

   node1    5       User:domain\user       Access denied by explicit ACE
                    Security Style:unix
                    Path:/dir1/
   ```

Modificar filtros de seguimiento de seguridad

Si desea cambiar los parámetros de filtro opcionales utilizados para determinar qué eventos de acceso se rastrean, puede modificar los filtros de seguimiento de seguridad existentes.

Acerca de esta tarea

Debe identificar el filtro de seguimiento de seguridad que desea modificar especificando el nombre de la máquina virtual de almacenamiento (SVM) en la que se aplica el filtro y el número de índice del filtro. Puede modificar todos los parámetros de filtro opcionales.

Pasos

1. Modificar un filtro de seguimiento de seguridad:

   `vserver security trace filter modify -vserver vserver_name -index index_numberfilter_parameters`

   - `vserver_name` Es el nombre de la SVM en la que desea aplicar un filtro de seguimiento de seguridad.
   - `index_number` es el número de índice que desea aplicar al filtro. Los valores permitidos para este parámetro son de 1 a 10.
   - `filter_parameters` es una lista de parámetros de filtro opcionales.

2. Compruebe la entrada del filtro de seguimiento de seguridad:

```
vserver security trace filter show -vserver vserver_name -index index_number
```

Ejemplo

El siguiente comando modifica el filtro de seguimiento de seguridad con el número de índice 1. El filtro realiza un seguimiento de los eventos de cualquier usuario que acceda a un archivo con una ruta de acceso compartido `\\server\share1\dir1\dir2\file.txt` Desde cualquier dirección IP. El filtro utiliza una ruta completa para el `-path` opción. Los seguimientos de filtro permiten y niegan eventos:

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                                Vserver: vs1
                           Filter Index: 1
             Client IP Address to Match: -
                                   Path: /dir1/dir2/file.txt
                     Windows User Name: -
                        UNIX User Name: -
                    Trace Allow Events: yes
                        Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

Elimine filtros de seguimiento de seguridad

Si ya no necesita una entrada de filtro de seguimiento de seguridad, puede eliminarla. Debido a que puede tener un máximo de 10 filtros de seguimiento de seguridad por máquina virtual de almacenamiento (SVM), al eliminar filtros innecesarios, podrá crear nuevos filtros si llegó al máximo.

Acerca de esta tarea

Para identificar de forma única el filtro de seguimiento de seguridad que desea eliminar, debe especificar lo siguiente:

- Nombre de la SVM a la que se aplica el filtro de seguimiento
- El número de índice del filtro de seguimiento

Pasos

1. Identifique el número de índice de filtro de la entrada del filtro de seguimiento de seguridad que desea eliminar:

   ```
   vserver security trace filter show -vserver vserver_name

   vserver security trace filter show -vserver vs1
   ```

```
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

2. Utilizando la información del número de índice de filtro del paso anterior, elimine la entrada de filtro:

   ```
   vserver security trace filter delete -vserver vserver_name -index index_number
   ```

   ```
   vserver security trace filter delete -vserver vs1 -index 1
   ```

3. Compruebe que la entrada del filtro de seguimiento de seguridad se ha eliminado:

   ```
   vserver security trace filter show -vserver vserver_name
   ```

   ```
   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

Eliminar registros de rastreo de seguridad

Después de terminar de utilizar un registro de seguimiento de filtro para verificar la seguridad de acceso a archivos o para solucionar problemas de acceso de clientes SMB o NFS, puede eliminar el registro de seguimiento de seguridad del registro de seguimiento de seguridad.

Acerca de esta tarea

Para poder eliminar un registro de seguimiento de seguridad, debe conocer el número de secuencia del registro.

> Cada máquina virtual de almacenamiento (SVM) puede almacenar un máximo de 128 registros de seguimiento. Si se alcanza el máximo en la SVM, los registros de seguimiento más antiguos se eliminan automáticamente a medida que se añaden otros nuevos. Si no desea eliminar manualmente los registros de seguimiento de esta SVM, es posible eliminar automáticamente ONTAP los resultados de rastros más antiguos después de alcanzar el máximo para hacer espacio para nuevos resultados.

Pasos

1. Identifique el número de secuencia del registro que desea eliminar:

   ```
   vserver security trace trace-result show -vserver vserver_name -instance
   ```

2. Elimine el registro de seguimiento de seguridad:

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name -seqnum integer

   vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
   999
   ```

   - `-node node_name` es el nombre del nodo de clúster en el que se produjo el evento de seguimiento de permisos que desea eliminar.

     Este es un parámetro obligatorio.

   - `-vserver vserver_name` Es el nombre de la SVM donde se produjo el evento de seguimiento de permisos que desea eliminar.

     Este es un parámetro obligatorio.

   - `-seqnum integer` es el número de secuencia del evento de registro que se desea eliminar.

     Este es un parámetro obligatorio.

Elimine todos los registros de rastreo de seguridad

Si no desea conservar ninguno de los registros de seguimiento de seguridad existentes, puede eliminar todos los registros de un nodo con un único comando.

Paso

1. Eliminar todos los registros de rastreo de seguridad:

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name *
   ```

   - `-node node_name` es el nombre del nodo de clúster en el que se produjo el evento de seguimiento de permisos que desea eliminar.
   - `-vserver vserver_name` Es el nombre de la máquina virtual de almacenamiento (SVM) donde se produjo el evento de seguimiento de permisos que desea eliminar.

Interpretar los resultados de las trazas de seguridad

Los resultados del seguimiento de seguridad proporcionan el motivo por el que se permitía o denegaba una solicitud. Salida muestra el resultado como una combinación de la razón por la que se permite o deniega el acceso y la ubicación dentro de la ruta de comprobación de acceso en la que se permite o se deniega el acceso. Puede utilizar los resultados para aislar e identificar por qué se permiten o no acciones.

Búsqueda de información acerca de las listas de tipos de resultados y detalles de filtro

Puede encontrar las listas de tipos de resultados y detalles de filtro que se pueden incluir en los resultados del rastreo de seguridad en las páginas man de `vserver security trace trace-result show` comando.

Ejemplo de resultado de la `Reason` en un `Allow` tipo de resultado

A continuación se muestra un ejemplo del resultado de la `Reason` campo que aparece en el registro de resultados de seguimiento en un `Allow` tipo de resultado:

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

Ejemplo de resultado de la `Reason` en un `Allow` tipo de resultado

A continuación se muestra un ejemplo del resultado de la `Reason` campo que aparece en el registro de resultados de seguimiento en un `Deny` tipo de resultado:

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

Ejemplo de resultado de la `Filter details` campo

A continuación se muestra un ejemplo del resultado de la `Filter details` campo del registro de resultados de seguimiento, que enumera el estilo de seguridad efectivo del sistema de archivos que contiene archivos y carpetas que coinciden con los criterios de filtro:

```
Security Style: MIXED and ACL
```

Dónde encontrar información adicional

Una vez que haya probado correctamente el acceso al cliente SMB, puede ejecutar la configuración avanzada de SMB o añadir acceso SAN. Una vez que haya probado correctamente el acceso al cliente NFS, puede ejecutar una configuración de NFS avanzada o añadir acceso SAN. Una vez completado el acceso al protocolo, debe proteger el volumen raíz de la SVM.

Configuración de SMB

Puede configurar el acceso SMB además utilizando lo siguiente:

- "Gestión de SMB"

Describe cómo configurar y gestionar el acceso a archivos mediante el protocolo SMB.

- "Informe técnico de NetApp 4191: Guía de mejores prácticas para servicios de archivos de Windows para Clustered Data ONTAP 8.2"

  Proporciona una breve descripción general de la implementación de SMB y otras funciones de servicios de archivos Windows con recomendaciones e información básica sobre solución de problemas para ONTAP.

- "Informe técnico de NetApp 3740: Protocolo CIFS de última generación de SMB 2 en Data ONTAP"

  Describe las funciones de SMB 2, los detalles de configuración y su implementación en ONTAP.

Configuración de NFS

Puede configurar el acceso NFS de forma adicional utilizando lo siguiente:

- "Gestión de NFS"

  Describe cómo configurar y gestionar el acceso a archivos mediante el protocolo NFS.

- "Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS"

  Sirve de guía de funcionamiento de NFSv3 y NFSv4 y ofrece una descripción general del sistema operativo de ONTAP haciendo hincapié en NFSv4.

- "Informe técnico de NetApp 4668: Guía de prácticas recomendadas de servicios de nombres"

  Proporciona una lista completa de prácticas recomendadas, límites, recomendaciones y consideraciones a la hora de configurar archivos de LDAP, NIS, DNS y usuarios locales y de grupos para fines de autenticación.

- "Informe técnico de NetApp 4616: Kerberos de NFS en ONTAP con Microsoft Active Directory"
- "Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP"
- "Informe técnico de NetApp 3580: Guía de mejoras y prácticas recomendadas de NFSv4: Implementación de Data ONTAP"

  Describe las prácticas recomendadas que se deben seguir mientras implementa componentes de NFSv4 en clientes AIX, Linux o Solaris conectados a sistemas que ejecutan ONTAP.

Protección de volúmenes raíz

Después de configurar los protocolos en la SVM, debe asegurarse de que su volumen raíz esté protegido:

- "Protección de datos"

  Describe cómo crear un reflejo de uso compartido de carga para proteger el volumen raíz de SVM, que es una práctica recomendada por NetApp para SVM habilitadas para NAS. También describe cómo recuperarse rápidamente de fallos o pérdidas de volúmenes mediante la promoción del volumen raíz de SVM desde un reflejo de uso compartido de carga.