Acceso NFS seguro mediante políticas de exportación

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Acceso NFS seguro mediante políticas de exportación

Cómo las políticas de exportación controlan el acceso de los clientes a volúmenes o qtrees

Las políticas de exportación contienen una o varias *reglas de exportación* que procesan cada solicitud de acceso de cliente. El resultado del proceso determina si se deniega o se concede acceso al cliente y qué nivel de acceso. Para que los clientes accedan a los datos, debe haber una política de exportación con reglas de exportación en la máquina virtual de almacenamiento (SVM).

Se asocia exactamente una política de exportación a cada volumen o qtree para configurar el acceso de los clientes al volumen o qtree. La SVM puede contener varias políticas de exportación. Esto le permite hacer lo siguiente para las SVM con varios volúmenes o qtrees:

- Asigne diferentes políticas de exportación a cada volumen o qtree de la SVM para controlar el acceso de cliente individual a cada volumen o qtree de la SVM.
- Asigne la misma política de exportación a varios volúmenes o qtrees de la SVM para un control de acceso del cliente idéntico sin que tenga que crear una nueva política de exportación para cada volumen o qtree.

Si un cliente realiza una solicitud de acceso que no está permitida por la política de exportación aplicable, la solicitud falla con un mensaje de permiso denegado. Si un cliente no coincide con ninguna regla de la política de exportación, se deniega el acceso. Si una política de exportación está vacía, se deniegan implícitamente todos los accesos.

Puede modificar dinámicamente una política de exportación en un sistema que ejecuta ONTAP.

Política de exportación predeterminada para las SVM

Cada SVM tiene una política de exportación predeterminada que no contiene reglas. Para que los clientes puedan acceder a los datos en la SVM, debe haber una política de exportación con reglas. Cada volumen FlexVol que contiene la SVM debe estar asociado a una política de exportación.

Cuando se crea una SVM, el sistema de almacenamiento crea automáticamente una política de exportación predeterminada llamada `default` Para el volumen raíz de la SVM. Debe crear una o varias reglas para la política de exportación predeterminada para que los clientes puedan acceder a los datos de la SVM. También puede crear una política de exportación personalizada con reglas. Puede modificar y cambiar el nombre de la política de exportación predeterminada, pero no puede eliminar la política de exportación predeterminada.

Cuando se crea un volumen FlexVol en la SVM que contiene, el sistema de almacenamiento crea el volumen y asocia el volumen con la política de exportación predeterminada para el volumen raíz de la SVM. De manera predeterminada, cada volumen creado en la SVM está asociado con la política de exportación predeterminada para el volumen raíz. Puede usar la política de exportación predeterminada para todos los volúmenes contenidos en la SVM, o bien puede crear una política de exportación única para cada volumen. Es posible asociar varios volúmenes con la misma política de exportación.

Cómo funcionan las reglas de exportación

Las reglas de exportación son los elementos funcionales de una política de exportación. Las reglas de exportación coinciden con las solicitudes de acceso de los clientes a un volumen con los parámetros específicos que se configuran para determinar cómo se manejan las solicitudes de acceso de los clientes.

La política de exportación debe contener al menos una regla de exportación para permitir el acceso a los clientes. Si una política de exportación contiene más de una regla, se procesan las reglas en el orden en que aparecen en la política de exportación. El orden de las reglas viene determinado por el número de índice de reglas. Si una regla coincide con un cliente, se utilizan los permisos de esa regla y no se procesan otras reglas. Si no hay reglas que coincidan, se deniega el acceso al cliente.

Puede configurar reglas de exportación para determinar los permisos de acceso de clientes con los siguientes criterios:

- El protocolo de acceso a archivos que utiliza el cliente para enviar la solicitud, por ejemplo, NFSv4 o SMB.
- Un identificador de cliente, por ejemplo, un nombre de host o una dirección IP.

  El tamaño máximo de `-clientmatch` el campo tiene 4096 caracteres.

- Tipo de seguridad utilizado por el cliente para autenticar, por ejemplo, Kerberos v5, NTLM o AUTH_SYS.

Si una regla especifica varios criterios, el cliente debe coincidir con todos ellos para que se aplique la regla.

> A partir de ONTAP 9.3, puede habilitar la comprobación de la configuración de la política de exportación como un trabajo en segundo plano que registra cualquier infracción de reglas en una lista de reglas de error. La `vserver export-policy config-checker` los comandos invocan al comprobador y muestran los resultados, que se pueden utilizar para verificar la configuración y eliminar reglas erróneas de la directiva.
>
> Los comandos solo validan la configuración de exportación para los nombres de host, grupos de red y usuarios anónimos.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La solicitud de acceso del cliente se envía mediante el protocolo NFSv3 y el cliente tiene la dirección IP 10.1.17.37.

Aunque el protocolo de acceso del cliente coincida, la dirección IP del cliente se encuentra en una subred diferente de la especificada en la regla de exportación. Por lo tanto, la coincidencia de cliente falla y esta regla no se aplica a este cliente.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La solicitud de acceso del cliente se envía con el protocolo NFSv4 y el cliente tiene la dirección IP 10,1.16,54.

El protocolo de acceso del cliente coincide y la dirección IP del cliente se encuentra en la subred especificada. Por lo tanto, la coincidencia de cliente es correcta y esta regla se aplica a este cliente. El cliente obtiene acceso de lectura y escritura independientemente de su tipo de seguridad.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

El cliente n.o 1 tiene la dirección IP 10.1.16.207, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El protocolo de acceso del cliente y la dirección IP coinciden con los dos clientes. El parámetro de solo lectura permite un acceso de solo lectura a todos los clientes independientemente del tipo de seguridad con el que se autentiquen. Por lo tanto, ambos clientes obtienen acceso de solo lectura. Sin embargo, sólo el cliente #1 obtiene acceso de lectura y escritura porque utilizó el tipo de seguridad aprobado Kerberos v5 para autenticar. El cliente n.o 2 no obtiene acceso de lectura/escritura.

Administrar clientes con un tipo de seguridad sin lista

Cuando un cliente se presenta a sí mismo con un tipo de seguridad que no aparece en un parámetro de acceso de una regla de exportación, tiene la opción de denegar el acceso al cliente o asignarlo al ID de usuario anónimo en su lugar mediante la opción `none` en el parámetro access.

Es posible que un cliente se presente a sí mismo con un tipo de seguridad que no aparece en un parámetro de acceso porque se autentica con un tipo de seguridad diferente o que no se haya autenticado en absoluto (tipo de seguridad AUTH_NONE). De forma predeterminada, al cliente se le deniega automáticamente el acceso a ese nivel. Sin embargo, puede agregar la opción `none` al parámetro access. Como resultado, los clientes con un estilo de seguridad no enumerado se asignan al ID de usuario anónimo en su lugar. La `-anon` Parámetro determina qué ID de usuario se asigna a esos clientes. El ID de usuario especificado para `-anon` el parámetro debe ser un usuario válido configurado con los permisos que considere apropiados para el usuario anónimo.

Valores válidos para `-anon` intervalo de parámetros desde `0` para `65535`.

ID de usuario asignado a. `-anon`	Tratamiento resultante de las solicitudes de acceso de los clientes
`0 - 65533`	La solicitud de acceso de cliente se asigna al ID de usuario anónimo y obtiene acceso en función de los permisos configurados para este usuario.
`65534`	La solicitud de acceso de cliente no se asigna al usuario y obtiene acceso en función de los permisos configurados para este usuario. Este es el valor predeterminado.
`65535`	La solicitud de acceso de cualquier cliente se deniega cuando se asigna a este ID y el cliente se presenta con el tipo de seguridad AUTH_NONE. La solicitud de acceso de los clientes con ID de usuario 0 se deniega cuando se asigna a este ID y el cliente se presenta a sí mismo con cualquier otro tipo de seguridad.

Al utilizar la opción `none`, es importante recordar que el parámetro de sólo lectura se procesa primero. Tenga en cuenta las siguientes directrices al configurar reglas de exportación para clientes con tipos de seguridad no listados:

Incluye solo lectura `none`	Incluye lectura y escritura `none`	Acceso resultante para clientes con tipos de seguridad no listados
No	No	Denegada
No	Sí	Denegado porque sólo lectura se procesa primero
Sí	No	Sólo lectura como anónimo
Sí	Sí	Lectura y escritura como anónimo

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

El cliente n.o 1 tiene la dirección IP 10.1.16.207, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El cliente #3 tiene la dirección IP 10.1.16.234, envía una solicitud de acceso con el protocolo NFSv3 y no se autentica (es decir, el tipo de seguridad AUTH_NONE).

El protocolo de acceso del cliente y la dirección IP coinciden con los tres clientes. El parámetro de sólo lectura permite el acceso de sólo lectura a clientes con su propio ID de usuario que se autentica con AUTH_SYS. El parámetro de sólo lectura permite el acceso de sólo lectura como usuario anónimo con ID de usuario 70 a clientes autenticados mediante cualquier otro tipo de seguridad. El parámetro de lectura y escritura permite acceso de lectura y escritura a cualquier tipo de seguridad, pero en este caso solo se aplica a los clientes ya filtrados por la regla de solo lectura.

Por lo tanto, los clientes #1 y #3 obtienen acceso de lectura y escritura sólo como el usuario anónimo con ID de usuario 70. El cliente #2 obtiene acceso de lectura y escritura con su propio ID de usuario.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

El cliente n.o 1 tiene la dirección IP 10.1.16.207, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El cliente #3 tiene la dirección IP 10.1.16.234, envía una solicitud de acceso con el protocolo NFSv3 y no se autentica (es decir, el tipo de seguridad AUTH_NONE).

El protocolo de acceso del cliente y la dirección IP coinciden con los tres clientes. El parámetro de sólo lectura permite el acceso de sólo lectura a clientes con su propio ID de usuario que se autentica con AUTH_SYS. El parámetro de sólo lectura permite el acceso de sólo lectura como usuario anónimo con ID de usuario 70 a clientes autenticados mediante cualquier otro tipo de seguridad. El parámetro de lectura y escritura permite el acceso de lectura y escritura sólo como el usuario anónimo.

Por lo tanto, el cliente #1 y el cliente #3 obtienen acceso de lectura y escritura sólo como el usuario anónimo con el ID de usuario 70. El cliente #2 obtiene acceso de sólo lectura con su propio ID de usuario pero se le deniega el acceso de lectura y escritura.

Cómo los tipos de seguridad determinan los niveles de acceso de los clientes

El tipo de seguridad con el que el cliente autenticado desempeña un rol especial en las

reglas de exportación. Debe entender la manera en que el tipo de seguridad determina los niveles de acceso que el cliente obtiene a un volumen o un qtree.

Los tres niveles de acceso posibles son los siguientes:

1. Solo lectura
2. Lectura-escritura
3. Superusuario (para clientes con ID de usuario 0)

Dado que el nivel de acceso por tipo de seguridad se evalúa en este orden, debe observar las siguientes reglas al construir parámetros de nivel de acceso en las reglas de exportación:

Para que un cliente obtenga el nivel de acceso…	**Estos parámetros de acceso deben coincidir con el tipo de seguridad del cliente…**
Usuario normal de solo lectura	Solo lectura (`-rorule`)
Lectura y escritura normal del usuario	Solo lectura (`-rorule`) y lectura y escritura (`-rwrule`)
Sólo lectura de superusuario	Solo lectura (`-rorule`) y. `-superuser`
Lectura y escritura de superusuario	Solo lectura (`-rorule`) y lectura y escritura (`-rwrule`) y. `-superuser`

A continuación, se muestran tipos de seguridad válidos para cada uno de estos tres parámetros de acceso:

- `any`
- `none`
- `never`

  Este tipo de seguridad no es válido para su uso con `-superuser` parámetro.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Al hacer coincidir el tipo de seguridad de un cliente con cada uno de los tres parámetros de acceso, hay tres resultados posibles:

Si el tipo de seguridad del cliente…	**A continuación, el cliente…**
Coincide con el especificado en el parámetro access.	Obtiene acceso para ese nivel con su propio ID de usuario.

Si el tipo de seguridad del cliente…	A continuación, el cliente…
No coincide con el especificado, pero el parámetro access incluye la opción `none`.	Obtiene acceso para ese nivel pero como usuario anónimo con el ID de usuario especificado por `-anon` parámetro.
No coincide con el especificado y el parámetro access no incluye la opción `none`.	No obtiene acceso para ese nivel. Esto no se aplica a `-superuser` parámetro porque siempre incluye `none` incluso cuando no se especifique.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys,krb5`
- `-superuser krb5`

El cliente #1 tiene la dirección IP 10.1.16.207, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El cliente #3 tiene la dirección IP 10.1.16.234, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y no se autentica (AUTH_NONE).

El protocolo de acceso del cliente y la dirección IP coinciden con los tres clientes. El parámetro de solo lectura permite el acceso de solo lectura a todos los clientes independientemente del tipo de seguridad. El parámetro de lectura y escritura permite acceder de lectura y escritura a clientes con su propio ID de usuario que se autentica con AUTH_SYS o Kerberos v5. El parámetro superusuario permite el acceso de superusuario a clientes con ID de usuario 0 que se autentiquen con Kerberos v5.

Por lo tanto, el cliente #1 obtiene acceso de lectura y escritura de superusuario porque coincide con los tres parámetros de acceso. El cliente #2 obtiene acceso de lectura y escritura, pero no acceso de superusuario. El cliente #3 obtiene acceso de sólo lectura pero no acceso de superusuario.

Administrar solicitudes de acceso de superusuario

Cuando configura políticas de exportación, debe tener en cuenta lo que desea que suceda si el sistema de almacenamiento recibe una solicitud de acceso de cliente con ID de usuario 0, lo que significa como superusuario y configure las reglas de exportación según corresponda.

En el mundo UNIX, un usuario con el ID de usuario 0 se conoce como superusuario, normalmente llamado root, que tiene derechos de acceso ilimitados en un sistema. El uso de privilegios de superusuario puede ser peligroso por varias razones, como la violación de la seguridad del sistema y de los datos.

De forma predeterminada, ONTAP asigna los clientes que presentan el ID de usuario 0 al usuario anónimo. Sin embargo, puede especificar el `- superuser` Parámetro en reglas de exportación para determinar cómo gestionar los clientes que presentan el ID de usuario 0 en función de su tipo de seguridad. A continuación, se muestran opciones válidas para el `-superuser` parámetro:

- `any`
- `none`

  Esta es la configuración predeterminada si no se especifica el `-superuser` parámetro.

- `krb5`
- `ntlm`
- `sys`

Hay dos maneras diferentes de manejar los clientes que presentan con ID de usuario 0, dependiendo de la `-superuser` configuración de parámetros:

Si la **`-superuser`** parámetro y tipo de seguridad del cliente…	A continuación, el cliente…
Coincidencia	Obtiene acceso de superusuario con ID de usuario 0.
No coinciden	Obtiene acceso como usuario anónimo con el ID de usuario especificado por `-anon` parámetro y sus permisos asignados. Esto es independientemente de si el parámetro de solo lectura o de lectura y escritura especifica la opción `none`.

Si un cliente presenta con el ID de usuario 0 para acceder a un volumen con estilo de seguridad NTFS y el `-superuser` el parámetro se establece en `none`, ONTAP utiliza la asignación de nombres del usuario anónimo para obtener las credenciales adecuadas.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

El cliente #1 tiene la dirección IP 10,1.16,207, tiene el ID de usuario 746, envía una solicitud de acceso mediante el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El protocolo de acceso del cliente y la dirección IP coinciden con los dos clientes. El parámetro de solo lectura

permite un acceso de solo lectura a todos los clientes independientemente del tipo de seguridad con el que se autentiquen. Sin embargo, sólo el cliente #1 obtiene acceso de lectura y escritura porque utilizó el tipo de seguridad aprobado Kerberos v5 para autenticar.

El cliente #2 no obtiene acceso de superusuario. En su lugar, se asigna a anónimo porque el `-superuser` no se ha especificado el parámetro. Esto significa que de forma predeterminada es `none` Y asigna automáticamente el ID de usuario 0 al anónimo. El cliente #2 sólo obtiene acceso de sólo lectura porque su tipo de seguridad no coincide con el parámetro de lectura y escritura.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

El cliente #1 tiene la dirección IP 10.1.16.207, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El protocolo de acceso del cliente y la dirección IP coinciden con los dos clientes. El parámetro de solo lectura permite un acceso de solo lectura a todos los clientes independientemente del tipo de seguridad con el que se autentiquen. Sin embargo, sólo el cliente #1 obtiene acceso de lectura y escritura porque utilizó el tipo de seguridad aprobado Kerberos v5 para autenticar. El cliente n.o 2 no obtiene acceso de lectura/escritura.

La regla de exportación permite el acceso de superusuario para clientes con ID de usuario 0. El cliente #1 obtiene acceso de superusuario porque coincide con el ID de usuario y el tipo de seguridad para los de sólo lectura y. `-superuser` parámetros. El cliente #2 no obtiene acceso de lectura-escritura o superusuario porque su tipo de seguridad no coincide con el parámetro de lectura-escritura o el `-superuser` parámetro. En su lugar, el cliente #2 está asignado al usuario anónimo, que en este caso tiene el ID de usuario 0.

Cómo utiliza ONTAP las cachés de la política de exportación

Para mejorar el rendimiento del sistema, ONTAP utiliza cachés locales para almacenar información como nombres de host y grupos de redes. De este modo, ONTAP puede procesar reglas de política de exportación más rápidamente que recuperar la información de fuentes externas. Comprender qué son las cachés y qué hacen puede ayudarlo a solucionar los problemas de acceso de los clientes.

Puede configurar políticas de exportación para controlar el acceso de los clientes a las exportaciones de NFS. Cada política de exportación contiene reglas y cada regla contiene parámetros que coincidan con los de los clientes que soliciten acceso. Algunos de estos parámetros requieren que ONTAP se ponga en contacto con un origen externo, como los servidores DNS o NIS, para resolver objetos como nombres de dominio, nombres

de host o grupos de red.

Estas comunicaciones con fuentes externas tardan una pequeña cantidad de tiempo. Para aumentar el rendimiento, ONTAP reduce la cantidad de tiempo que se necesita para resolver los objetos de reglas de políticas de exportación almacenando la información localmente en cada nodo en varias cachés.

Nombre de caché	Tipo de información almacenada
Acceso	Asignaciones de clientes a las correspondientes políticas de exportación
Nombre	Se asignan los nombres de usuario UNIX a los correspondientes ID de usuario UNIX
ID	Mapeos de ID de usuario de UNIX a ID de usuario de UNIX correspondientes e ID de grupo de UNIX ampliado
Host	Asignación de los nombres de host a las direcciones IP correspondientes
Grupo de red	Asignaciones de grupos de red a las direcciones IP correspondientes de los miembros
Showmount	Lista de directorios exportados desde el espacio de nombres de SVM

Si cambia información de los servidores de nombres externos de su entorno después de que ONTAP haya recuperado y almacenado localmente, es posible que las cachés contengan información obsoleta. Aunque las actualizaciones de ONTAP se actualizan automáticamente en caché tras ciertos periodos de tiempo, diferentes cachés tienen tiempos y algoritmos de caducidad y actualización diferentes.

Otra posible razón para que las cachés contengan información obsoleta es cuando ONTAP intenta actualizar la información almacenada en caché pero encuentra un error al intentar comunicarse con servidores de nombres. Si esto sucede, ONTAP sigue usando la información actualmente almacenada en la caché local para evitar que se produzca una interrupción del cliente.

Como resultado, las solicitudes de acceso a clientes que se supone que tienen éxito pueden fallar y las solicitudes de acceso de clientes que se supone que fallan se pueden realizar correctamente. Puede ver y purgar manualmente algunas de las cachés de políticas de exportación al solucionar los problemas de acceso de los clientes.

Cómo funciona la caché de acceso

ONTAP usa una caché de acceso para almacenar los resultados de la evaluación de las reglas de política de exportación para las operaciones de acceso de los clientes a un volumen o un qtree. Esto genera mejoras en el rendimiento porque la información se puede recuperar mucho más rápido de la caché de acceso que pasar por el proceso de evaluación de las reglas de la política de exportación cada vez que un cliente envía una solicitud de I/O.

Siempre que un cliente NFS envía una solicitud de I/o para acceder a los datos de un volumen o un qtree, ONTAP debe evaluar cada solicitud de I/o para determinar si desea conceder o denegar la solicitud de I/O. Esta evaluación implica la comprobación de cada regla de política de exportación de la política de exportación asociada con el volumen o el qtree. Si la ruta al volumen o qtree implica cruzar uno o más puntos de unión, puede ser necesario realizar esta comprobación en busca de varias políticas de exportación por la ruta.

Tenga en cuenta que esta evaluación se produce para cada solicitud de I/o que se envía desde un cliente NFS, como operaciones de lectura, escritura, lista, copia y otras, y no solo para solicitudes de montaje iniciales.

Una vez que ONTAP ha identificado las reglas de política de exportación aplicables y ha decidido si permitir o denegar la solicitud, ONTAP creará una entrada en la caché de acceso para almacenar dicha información.

Cuando un cliente NFS envía una solicitud de I/o, ONTAP señala la dirección IP del cliente, el ID de la SVM y la política de exportación asociada con el volumen o qtree de destino, y, primero, comprueba la caché de acceso para ver si existe una entrada correspondiente. Si existe una entrada coincidente en la caché de acceso, ONTAP utiliza la información almacenada para permitir o denegar la solicitud de E/S. Si no existe una entrada coincidente, ONTAP pasa por el proceso normal de evaluación de todas las reglas de política aplicables como se ha explicado anteriormente.

Las entradas de la caché de acceso que no se utilizan activamente no se actualizan. Esto reduce la comunicación innecesaria y innecesaria con servicios de nombres externos.

La recuperación de la información de la caché de acceso es mucho más rápida que pasar por todo el proceso de evaluación de las reglas de política de exportación para cada solicitud de I/O. Por lo tanto, el uso de la caché de acceso mejora considerablemente el rendimiento, ya que reduce la sobrecarga de las comprobaciones del acceso de los clientes.

Cómo funciona el acceso a los parámetros de caché

Varios parámetros controlan los períodos de actualización de las entradas de la caché de acceso. Comprender cómo funcionan estos parámetros le permite modificarlos para ajustar la caché de acceso y equilibrar el rendimiento con lo reciente que es la información almacenada.

La caché de acceso almacena entradas que constan de una o varias reglas de exportación que se aplican a los clientes que intentan acceder a volúmenes o qtrees. Estas entradas se almacenan durante cierto tiempo antes de que se actualicen. El tiempo de actualización viene determinado por los parámetros de la caché de acceso y depende del tipo de entrada de la caché de acceso.

Puede especificar parámetros de caché de acceso para SVM individuales. Esto permite que los parámetros difieren de acuerdo con los requisitos de acceso de la SVM. Las entradas de la caché de acceso que no se utilizan activamente no se actualizan, lo que reduce la comunicación innecesaria y innecesaria con servicios de nombres externos.

Tipo de entrada de la caché de acceso	Descripción	Actualice el periodo en segundos

Entradas positivas	Acceso a las entradas de caché que no han dado lugar a una denegación de acceso a los clientes.	Mínimo: 300 Máximo: 86,400 El valor predeterminado es 3,600
Entradas negativas	Las entradas de caché de acceso que han dado lugar a una denegación de acceso a los clientes.	Mínimo: 60 Máximo: 86,400 El valor predeterminado es 3,600

Ejemplo

Un cliente NFS intenta acceder a un volumen de un clúster de. ONTAP coincide con el cliente con una regla de política de exportación y determina que el cliente obtiene acceso en función de la configuración de la regla de la política de exportación. ONTAP almacena la regla de política de exportación en la caché de acceso como una entrada positiva. De forma predeterminada, ONTAP mantiene la entrada positiva de la caché de acceso durante una hora (3,600 segundos) y, a continuación, actualiza automáticamente la entrada para mantener la información actualizada.

Para evitar que la caché de acceso se llene innecesariamente, hay un parámetro adicional para borrar las entradas existentes de la caché de acceso que no se han utilizado durante un determinado período de tiempo para decidir el acceso de cliente. Este `-harvest-timeout` el parámetro tiene un intervalo permitido de 60 a 2,592,000 segundos y un ajuste predeterminado de 86,400 segundos.

Quitar una política de exportación de un qtree

Si decide que ya no desea asignar una política de exportación específica a un qtree, puede eliminar la política de exportación modificando el qtree para que herede la política de exportación del volumen que lo contiene. Para ello, utilice `volume qtree modify` con el `-export-policy` parámetro y cadena de nombre vacía ("").

Pasos

1. Para quitar una política de exportación de un qtree, introduzca el siguiente comando:

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. Compruebe que el qtree se ha modificado en consecuencia:

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

Validar los ID de Qtree para operaciones de archivos de qtree

ONTAP puede realizar una validación adicional opcional de identificadores de qtree. Esta

validación garantiza que las solicitudes de operaciones de archivos cliente utilicen un identificador de qtree válido y que los clientes solo puedan mover archivos dentro del mismo qtree. Puede habilitar o deshabilitar esta validación modificando el `-validate -qtree-export` parámetro. Este parámetro está habilitado de forma predeterminada.

Acerca de esta tarea

Este parámetro solo es eficaz cuando se ha asignado una política de exportación directamente a uno o varios qtrees de la máquina virtual de almacenamiento (SVM).

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

Si desea que la validación de ID de qtree sea…	Introduzca el siguiente comando…
Activado	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
Deshabilitado	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Restricciones de la directiva de exportación y uniones anidadas para volúmenes FlexVol

Si ha configurado políticas de exportación para establecer una política menos restrictiva en una unión anidada, pero una política más restrictiva en una unión de nivel superior, puede que no se pueda acceder a la unión de nivel inferior.

Debe asegurarse de que las uniones de nivel superior tienen políticas de exportación menos restrictivas que las uniones de nivel inferior.