Comprenda FPolicy

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Comprenda FPolicy

Cuáles son las dos partes de la solución FPolicy

FPolicy es un marco de notificación del acceso a archivos que se utiliza para supervisar y gestionar los eventos de acceso a archivos en máquinas virtuales de almacenamiento (SVM) a través de soluciones de partners. Las soluciones de partners te ayudan a abordar diversos casos de uso, como la gobernanza de datos y el cumplimiento de normativas, la protección frente a ransomware y la movilidad de datos.

Las soluciones para partners incluyen soluciones de 3rd partes compatibles con NetApp y productos de NetApp Workload Security y Cloud Data Sense.

Una solución FPolicy consta de dos partes. El marco de FPolicy de ONTAP gestiona las actividades en el clúster y envía notificaciones a las aplicaciones asociadas (también conocidas como servidores FPolicy externos). Los servidores externos de FPolicy procesan notificaciones que envía FPolicy de ONTAP para cumplir los casos de uso de clientes.

El marco de ONTAP crea y mantiene la configuración de FPolicy, supervisa eventos de archivos y envía notificaciones a servidores de FPolicy externos. FPolicy de ONTAP proporciona la infraestructura que permite la comunicación entre servidores FPolicy externos y nodos de máquinas virtuales de almacenamiento (SVM).

El marco de FPolicy se conecta a servidores de FPolicy externos y envía notificaciones para ciertos eventos del sistema de archivos a los servidores FPolicy cuando estos eventos se producen como resultado del acceso de los clientes. Los servidores FPolicy externos procesan las notificaciones y envían respuestas de nuevo al nodo. Lo que ocurre como resultado del procesamiento de la notificación depende de la aplicación y si la comunicación entre el nodo y los servidores externos es asíncrona o síncrona.

Qué son las notificaciones síncronas y asíncronas

FPolicy envía notificaciones a servidores de FPolicy externos a través de la interfaz de FPolicy. Las notificaciones se envían en modo síncrono o asíncrono. El modo de notificación determina lo que hace ONTAP después de enviar notificaciones a los servidores FPolicy.

- **Notificaciones Asynchronous**

  Con notificaciones asíncronas, el nodo no espera una respuesta del servidor FPolicy, lo cual mejora el rendimiento general del sistema. Este tipo de notificación es adecuado para aplicaciones en las que el servidor FPolicy no requiere que se realice ninguna acción como resultado de la evaluación de notificaciones. Por ejemplo, las notificaciones asíncronas se usan cuando el administrador de la máquina virtual de almacenamiento (SVM) desea supervisar y auditar la actividad de acceso a archivos.

  Si un servidor de FPolicy que funciona en modo asíncrono experimenta una interrupción de la red, las notificaciones de FPolicy generadas durante la interrupción se almacenan en el nodo de almacenamiento. Cuando el servidor FPolicy vuelve a estar conectado, recibe alertas de las notificaciones almacenadas y pueden recogerlas del nodo de almacenamiento. El tiempo que las notificaciones se pueden almacenar durante una interrupción se puede configurar hasta 10 minutos.

  A partir de ONTAP 9.14.1, FPolicy permite configurar un almacén persistente para capturar eventos de acceso a archivos para políticas asíncronas no obligatorias en la SVM. Los almacenes persistentes

pueden ayudar a desacoplar el procesamiento de I/O del cliente del procesamiento de notificaciones de FPolicy para reducir la latencia del cliente. No se admiten las configuraciones síncronas (obligatorias o no obligatorias) y asíncronas obligatorias.

- **Notificaciones sinc**

  Cuando se configura para ejecutarse en modo síncrono, el servidor de FPolicy debe reconocer todas las notificaciones antes de permitir que continúe la operación del cliente. Este tipo de notificación se utiliza cuando se requiere una acción basada en los resultados de la evaluación de la notificación. Por ejemplo, las notificaciones síncronas se utilizan cuando el administrador de SVM desea permitir o denegar solicitudes en función de los criterios especificados en el servidor de FPolicy externo.

Aplicaciones síncronas y asíncronas

Existen muchos usos posibles para las aplicaciones de FPolicy, tanto asíncronas como síncronas.

Las aplicaciones asíncronas son aquellas en las que el servidor de FPolicy externo no altera el acceso a los archivos o directorios ni modifica los datos de la máquina virtual de almacenamiento (SVM). Por ejemplo:

- Acceso a archivos y registro de auditorías
- Gestión de recursos de almacenamiento

Las aplicaciones síncronas son aquellas en las que el acceso a los datos se altera o el servidor FPolicy externo modifica los datos. Por ejemplo:

- Gestión de cuotas
- Bloqueo de acceso a archivos
- Archivado de ficheros y gestión del almacenamiento jerárquico
- Servicios de cifrado y descifrado
- Servicios de compresión y descompresión

Almacenes persistentes de FPolicy

A partir de ONTAP 9.14.1, FPolicy permite configurar un almacén persistente para capturar eventos de acceso a archivos para políticas asíncronas no obligatorias en la SVM. Los almacenes persistentes pueden ayudar a desacoplar el procesamiento de I/O del cliente del procesamiento de notificaciones de FPolicy para reducir la latencia del cliente. No se admiten las configuraciones síncronas (obligatorias o no obligatorias) y asíncronas obligatorias.

Esta función solo está disponible en el modo externo de FPolicy. La aplicación asociada que utilice necesita admitir esta función. Debe trabajar con su partner para garantizar que esta configuración de FPolicy sea compatible.

Mejores prácticas

Los administradores de clústeres deben configurar un volumen para el almacén persistente en cada SVM en la que FPolicy esté habilitado. Cuando se configura, un almacén persistente captura todos los eventos de FPolicy que coinciden, que se procesan posteriormente en la canalización de FPolicy y se envían al servidor externo.

El almacén persistente permanece igual que cuando se recibió el último evento cuando se produce un reinicio inesperado o FPolicy se deshabilita y vuelve a habilitar. Tras una operación de toma de control, el nodo asociado almacenará y procesará los nuevos eventos. Tras una operación de devolución, el almacén persistente reanuda el procesamiento de todos los eventos sin procesar que pudieran permanecer desde el momento en que se produjo la toma de control del nodo. Los eventos en directo tendrán prioridad sobre los eventos no procesados.

Si el volumen de almacenamiento persistente se mueve de un nodo a otro en la misma SVM, las notificaciones que aún están por procesar también se moverán al nuevo nodo. Deberá volver a ejecutar el `fpolicy persistent-store create` comando en cualquiera de los nodos después de mover el volumen para garantizar que la notificación pendiente se entregue al servidor externo.

El volumen de almacenamiento persistente se configura por SVM. Para cada SVM con FPolicy, deberá crear un volumen de almacenamiento persistente.

Cree el volumen de almacenamiento persistente en el nodo con LIF que esperan que Fpolicy supervise el tráfico máximo.

Si las notificaciones acumuladas en el almacén persistente superan el tamaño del volumen aprovisionado, FPolicy comenzará a borrar la notificación entrante con los mensajes EMS adecuados.

El nombre del volumen de almacenamiento persistente y la ruta de unión especificada en el momento de la creación del volumen deben coincidir.

Establezca la política de Snapshot en `none` para ese volumen en lugar de `default`. De este modo se garantiza que no haya ninguna restauración accidental de la instantánea que provoque la pérdida de eventos actuales y que se evite un posible procesamiento de eventos duplicados.

Haga que el volumen de almacenamiento persistente no sea accesible para el acceso del protocolo de usuario externo (CIFS/NFS) y evite daños o eliminación accidentales de los registros de eventos persistentes. Para lograr esto, después de habilitar FPolicy, desmonte el volumen en ONTAP para eliminar la ruta de unión, esto hace que sea inaccesible para el acceso al protocolo de usuario.

Para obtener más información, consulte "Crear almacenes persistentes".

Tipos de configuración de FPolicy

Existen dos tipos de configuración básicos de FPolicy. Una configuración usa servidores FPolicy externos para procesar y actuar según las notificaciones. La otra configuración no utiliza servidores de FPolicy externos; en su lugar, utiliza el servidor FPolicy nativo interno de ONTAP para bloquear archivos fácilmente según extensiones.

- **Configuración del servidor FPolicy externo**

  La notificación se envía al servidor FPolicy, que examina la solicitud y aplica reglas para determinar si el nodo debe permitir la operación de archivos solicitada. Para las políticas síncronas, el servidor de FPolicy envía una respuesta al nodo para permitir o bloquear la operación de archivos solicitada.

- **Configuración del servidor FPolicy nativo**

  La notificación se ha seleccionado internamente. La solicitud se permite o se deniega según la configuración de extensión de archivo configurada en el ámbito de FPolicy.

  Nota: Las solicitudes de extensión de archivo denegadas no se registran.

Cuándo crear una configuración de FPolicy nativa

Las configuraciones nativas de FPolicy utilizan el motor de FPolicy interno de ONTAP para supervisar y bloquear las operaciones de archivos según la extensión del archivo. Esta solución no requiere servidores FPolicy externos (servidores FPolicy). El uso de una configuración nativa de bloqueo de archivos es apropiado cuando se necesita esta sencilla solución.

El bloqueo de archivos nativo permite supervisar cualquier operación de archivo que coincida con eventos de operación y filtrado configurados y, a continuación, denegar el acceso a archivos con extensiones específicas. Esta es la configuración predeterminada.

Esta configuración proporciona un medio para bloquear el acceso a los archivos basándose únicamente en la extensión del archivo. Por ejemplo, para bloquear los archivos que contienen `mp3` extensiones, puede configurar una directiva para proporcionar notificaciones para ciertas operaciones con extensiones de archivo de destino de `mp3`. La directiva está configurada para denegar `mp3` peticiones de archivo para operaciones que generan notificaciones.

Lo siguiente se aplica a las configuraciones nativas de FPolicy:

- También se admite el mismo conjunto de filtros y protocolos compatibles con el tramado de archivos basado en servidor de FPolicy para el bloqueo de archivos nativo.
- El bloqueo de archivos nativo y las aplicaciones de filtrado de archivos basadas en servidor FPolicy se pueden configurar al mismo tiempo.

  Para ello, es posible configurar dos políticas de FPolicy independientes para la máquina virtual de almacenamiento (SVM), con una configurada para el bloqueo de archivos nativo y otra para el filtrado de archivos basado en servidor de FPolicy.

- La función nativa de bloqueo de archivos sólo controla los archivos basándose en las extensiones y no en el contenido del archivo.
- En el caso de enlaces simbólicos, el bloqueo de archivos nativos utiliza la extensión de archivo del archivo raíz.

Más información acerca de "FPolicy: Bloqueo de archivos nativo".

Cuándo crear una configuración que utilice servidores de FPolicy externos

Las configuraciones de FPolicy que utilizan servidores de FPolicy externos para procesar y gestionar notificaciones proporcionan soluciones sólidas para casos de uso, en los que se necesite algo más que un simple bloqueo de archivos según la extensión de archivos.

Debe crear una configuración que utilice servidores de FPolicy externos cuando desee realizar tareas como supervisar y registrar eventos de acceso a archivos, proporcionar servicios de cuotas, realizar bloqueo de archivos según criterios distintos a extensiones de archivos simples, proporcionar servicios de migración de datos mediante aplicaciones de gestión del almacenamiento jerárquicas, O bien ofrece un conjunto detallado de políticas que supervisan solo un subconjunto de datos de la máquina virtual de almacenamiento (SVM).

Las funciones que desempeñan los componentes del clúster con la implementación de FPolicy

El clúster, las máquinas virtuales de almacenamiento (SVM) contenidas y las LIF de datos tienen un rol en una implementación de FPolicy.

- **cluster**

  El clúster contiene el marco de gestión de FPolicy y mantiene y gestiona información acerca de todas las configuraciones de FPolicy del clúster.

- **SVM**

  Una configuración de FPolicy se define a nivel de SVM. El alcance de la configuración es la SVM, y solo funciona en recursos de SVM. Una configuración de SVM no puede supervisar ni enviar notificaciones para las solicitudes de acceso a los archivos que se realicen para los datos que residen en otra SVM.

  Las configuraciones de FPolicy se pueden definir en la SVM de administrador. Después de definir las configuraciones en la SVM de administrador, pueden verse y utilizarse en todas las SVM.

- **LIF de datos**

  Las conexiones con los servidores FPolicy se realizan a través de LIF de datos que pertenecen a la SVM con la configuración de FPolicy. Los LIF de datos utilizados para estas conexiones pueden realizar la conmutación al respaldo de la misma manera que los LIF de datos utilizados para el acceso normal de los clientes.

Cómo funciona FPolicy con servidores de FPolicy externos

Una vez que se configura y se habilita FPolicy en la máquina virtual de almacenamiento (SVM), FPolicy se ejecuta en todos los nodos en los que participa la SVM. FPolicy es responsable de establecer y mantener conexiones con servidores FPolicy externos (servidores FPolicy), para el procesamiento de notificaciones y para gestionar mensajes de notificación hacia y desde los servidores FPolicy.

Además, como parte de la gestión de conexiones, FPolicy tiene las siguientes responsabilidades:

- Garantiza que la notificación de archivo fluya a través del LIF correcto hacia el servidor FPolicy.
- Garantiza que cuando varios servidores FPolicy están asociados a una política, el equilibrio de carga se lleva a cabo al enviar notificaciones a los servidores de FPolicy.
- Intenta restablecer la conexión cuando se interrumpe una conexión con un servidor FPolicy.
- Envía las notificaciones a los servidores de FPolicy a través de una sesión autenticada.
- Gestiona la conexión de datos de lectura directa establecida por el servidor FPolicy para atender las solicitudes del cliente cuando está habilitada la lectura de pasarela.

Cómo se utilizan los canales de control para la comunicación de FPolicy

FPolicy inicia una conexión de canal de control a un servidor FPolicy externo desde las LIF de datos de cada nodo que participa en una máquina virtual de almacenamiento (SVM). FPolicy utiliza canales de control para transmitir notificaciones de archivos; por lo tanto, un servidor FPolicy puede ver varias conexiones de canal de control en función de la topología de SVM.

Cómo se utilizan los canales de acceso a datos con privilegios para la comunicación síncrona

Con los casos de uso síncrono, el servidor de FPolicy accede a los datos que residen en la máquina virtual de

almacenamiento (SVM) a través de una ruta de acceso a los datos privilegiada. El acceso a través de la ruta privilegiada expone el sistema de archivos completo al servidor FPolicy. Puede acceder a los archivos de datos para recopilar información, para analizar archivos, leer archivos o escribir en archivos.

Debido a que el servidor FPolicy externo puede acceder a todo el sistema de archivos desde la raíz de la SVM a través del canal de datos con privilegios, la conexión de canal de datos con privilegios debe ser segura.

Cómo se utilizan las credenciales de conexión de FPolicy con canales de acceso a datos con privilegios

El servidor FPolicy realiza conexiones de acceso a datos con privilegios a nodos del clúster mediante una credencial de usuario de Windows específica que se guarda con la configuración de FPolicy. SMB es el único protocolo compatible para hacer una conexión con un canal de acceso a datos privilegiado.

Si el servidor FPolicy requiere acceso a datos con privilegios, deben cumplirse las siguientes condiciones:

- Debe habilitarse una licencia para SMB en el clúster.
- El servidor FPolicy debe ejecutarse con las credenciales configuradas en la configuración de FPolicy.

Al realizar una conexión de canal de datos, FPolicy utiliza la credencial para el nombre de usuario de Windows especificado. El acceso a los datos se realiza a través del recurso compartido ONTAP_ADMIN$ del administrador.

Qué significa otorgar credenciales de superusuario para acceso a datos con privilegios

ONTAP usa la combinación de la dirección IP y las credenciales de usuario configuradas en la configuración de FPolicy para otorgar credenciales de superusuario al servidor FPolicy.

El estado de superusuario otorga los siguientes privilegios cuando el servidor FPolicy acceda a los datos:

- Evite las comprobaciones de permisos

  El usuario evita las comprobaciones de los archivos y el acceso al directorio.

- Privilegios especiales de bloqueo

  ONTAP permite el acceso de lectura, escritura o modificación a cualquier archivo independientemente de los bloqueos existentes. Si el servidor FPolicy recibe bloqueos de rango de bytes en el archivo, se elimina inmediatamente los bloqueos existentes en el archivo.

- Omitir las comprobaciones de FPolicy

  El acceso no genera ninguna notificación de FPolicy.

Cómo gestiona FPolicy el procesamiento de políticas

Es posible que haya varias políticas de FPolicy asignadas a la máquina virtual de almacenamiento (SVM), cada una con una prioridad diferente. Para crear una configuración de FPolicy adecuada en la SVM, es importante comprender la forma en que FPolicy gestiona el procesamiento de políticas.

Cada solicitud de acceso a archivos se evalúa inicialmente para determinar qué directivas están supervisando este evento. Si se trata de un evento supervisado, la información acerca del evento supervisado junto con las políticas interesadas se transfiere a FPolicy donde se evalúa. Cada política se evalúa por orden de prioridad

asignada.

Al configurar las directivas, debe tener en cuenta las siguientes recomendaciones:

- Si desea que una directiva se evalúe siempre antes que otras directivas, configure dicha directiva con una prioridad más alta.
- Si el éxito de la operación de acceso a archivos solicitada en un evento supervisado es un requisito previo para una solicitud de archivo que se evalúa en relación con otra directiva, asigne una prioridad a la directiva que controla el éxito o el fallo de la primera operación de archivo.

  Por ejemplo, si una política gestiona la funcionalidad de archivado y restauración de archivos de FPolicy y una segunda política gestiona las operaciones de acceso a archivos en el archivo en línea, la directiva que gestiona la restauración de archivos debe tener una prioridad más alta para que el archivo se restaure antes de que se permita la operación gestionada por la segunda directiva.

- Si desea que se evalúen todas las directivas que puedan aplicarse a una operación de acceso a archivos, dé prioridad a las directivas síncronas.

Puede reorganizar las prioridades de directivas existentes modificando el número de secuencia de directivas. Sin embargo, para que FPolicy evalúe políticas en función del orden de prioridad modificado, debe deshabilitar y volver a habilitar la política con el número de secuencia modificado.

Qué es el proceso de comunicación entre el servidor FPolicy externo y el nodo

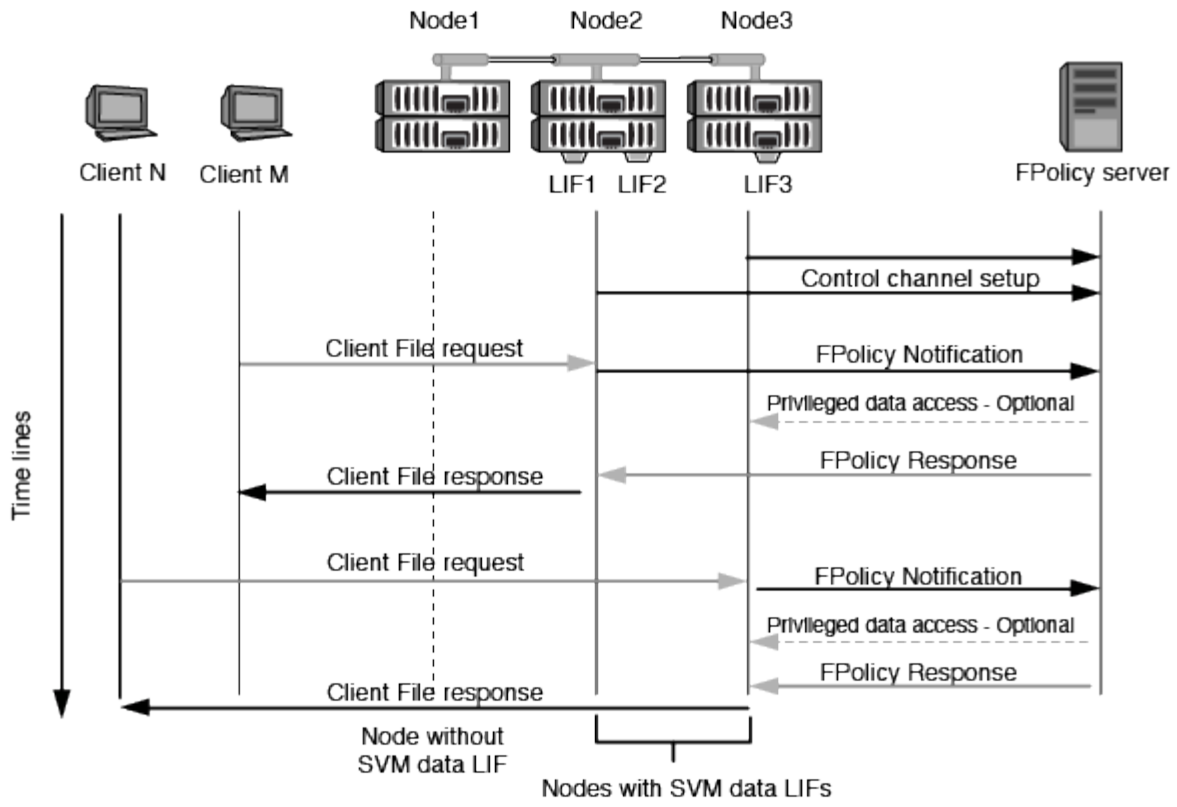
Para planificar correctamente la configuración de FPolicy, debe comprender cuál es el proceso de comunicación entre servidores FPolicy externos.

Cada nodo que participa en cada máquina virtual de almacenamiento (SVM) inicia una conexión con un servidor de FPolicy externo (servidor FPolicy) mediante TCP/IP. Las conexiones con los servidores FPolicy se configuran mediante LIF de datos de nodos; por lo tanto, un nodo participante solo puede configurar una conexión si el nodo tiene una LIF de datos operativa para la SVM.

Cada proceso de FPolicy en los nodos participantes intenta establecer una conexión con el servidor FPolicy cuando se habilite la política. Utiliza la dirección IP y el puerto del motor externo de FPolicy especificado en la configuración de directivas.

La conexión establece un canal de control desde cada uno de los nodos que participan en cada SVM al servidor FPolicy a través de la LIF de datos. Además, si las direcciones LIF de datos IPv4 e IPv6 están presentes en el mismo nodo participante, FPolicy intenta establecer conexiones tanto para IPv4 como IPv6. Por lo tanto, en una situación en la que la SVM se extiende por varios nodos o si hay direcciones IPv4 e IPv6 presentes, el servidor de FPolicy debe estar preparado para varias solicitudes de configuración de canal de control desde el clúster después de habilitar la política FPolicy en la SVM.

Por ejemplo, si un clúster tiene tres nodos (Node1, Node2 y Node3) y los LIF de datos de SVM se distribuyen en Node2 y Node3, los canales de control se inician solo desde Node2 y Node3, independientemente de la distribución de los volúmenes de datos. Supongamos que Node2 tiene dos LIF de datos (LIF1 y LIF2) que pertenecen a la SVM y que la conexión inicial es de LIF1. Si LIF1 falla, FPolicy intenta establecer un canal de control desde LIF2.



Cómo gestiona FPolicy la comunicación externa durante la migración LIF o la conmutación al nodo de respaldo

Los LIF de datos pueden migrarse a puertos de datos del mismo nodo o a puertos de datos de un nodo remoto.

Cuando se produce un error en una LIF de datos o se migra, se establece una nueva conexión de canal de control al servidor de FPolicy. A continuación, FPolicy puede volver a intentar solicitudes de clientes SMB y NFS que agoten el tiempo de espera, con el resultado de enviar nuevas notificaciones a los servidores de FPolicy externos. El nodo rechaza las respuestas del servidor de FPolicy frente a las solicitudes originales de SMB y NFS que han superado el tiempo de espera.

Cómo gestiona FPolicy la comunicación externa durante la conmutación al nodo de respaldo

Si el nodo del clúster que aloja los puertos de datos utilizados para la comunicación de FPolicy falla, ONTAP interrumpe la conexión entre el servidor de FPolicy y el nodo.

El impacto de la conmutación por error de clúster en el servidor FPolicy se puede mitigar configurando la política de conmutación por error para migrar el puerto de datos utilizado en la comunicación de FPolicy a otro nodo activo. Una vez finalizada la migración, se establece una nueva conexión con el nuevo puerto de datos.

Si la política de conmutación por error no está configurada para migrar el puerto de datos, el servidor FPolicy debe esperar a que se active el nodo fallido. Una vez que el nodo está en funcionamiento, se inicia una nueva conexión desde ese nodo con un nuevo ID de sesión.

El servidor FPolicy detecta conexiones rotas con el mensaje de protocolo Keep-alive. El tiempo de espera para purgar el ID de sesión se determina al configurar FPolicy. El tiempo de espera de mantenimiento activo predeterminado es de dos minutos.

Cómo funcionan los servicios de FPolicy en espacios de nombres de SVM

ONTAP proporciona un espacio de nombres de máquina virtual de almacenamiento unificado (SVM). Los volúmenes del clúster se unen entre sí por uniones para proporcionar un único sistema de archivos lógico. El servidor FPolicy conoce la topología de espacio de nombres y proporciona servicios FPolicy en todo el espacio de nombres.

El espacio de nombres es específico de la SVM y está contenido en ella; por lo tanto, solo se puede ver el espacio de nombres desde el contexto de la SVM. Los espacios de nombres tienen las siguientes características:

- Existe un espacio de nombres único en cada SVM, donde la raíz del espacio de nombres es el volumen raíz, representado en el espacio de nombres como barra diagonal (/).
- Todos los demás volúmenes tienen puntos de unión por debajo de la raíz (/).
- Las uniones del volumen son transparentes para los clientes.
- Una única exportación de NFS puede proporcionar acceso al espacio de nombres completo; de lo contrario, las políticas de exportación pueden exportar volúmenes específicos.
- Los recursos compartidos de SMB se pueden crear en el volumen o en qtrees dentro del volumen, o en cualquier directorio dentro del espacio de nombres.
- La arquitectura de espacio de nombres es flexible.

  A continuación se muestran ejemplos de arquitecturas de espacios de nombres típicas:

  - Un espacio de nombres con una única sucursal fuera de la raíz
  - Un espacio de nombres con varias sucursales fuera de la raíz
  - Un espacio de nombres con varios volúmenes sin ramificar de la raíz

Cómo la lectura de traspaso de FPolicy mejora la capacidad de uso para la gestión de almacenamiento jerárquica

La lectura de paso a través permite que el servidor FPolicy (funcionando como servidor de gestión de almacenamiento jerárquico (HSM) proporcione acceso de lectura a archivos sin tener que recuperar el archivo desde el sistema de almacenamiento secundario al sistema de almacenamiento primario.

Cuando un servidor FPolicy se configura para proporcionar HSM a archivos que residen en un servidor SMB, la migración de archivos basada en políticas se produce cuando los archivos se almacenan sin conexión en un almacenamiento secundario y solo queda un archivo stub en el almacenamiento principal. Aunque un archivo stub aparece como un archivo normal para los clientes, en realidad es un archivo sparse que tiene el mismo tamaño del archivo original. El archivo sparse tiene el bit de SMB sin conexión y apunta al archivo real que se ha migrado al almacenamiento secundario.

Normalmente, cuando se recibe una solicitud de lectura de un archivo sin conexión, el contenido solicitado debe volver a recuperarse en el almacenamiento principal y, a continuación, acceder a él a través del almacenamiento principal. La necesidad de recuperar los datos en el almacenamiento primario produce varios efectos no deseados. Entre los efectos no deseables se encuentra el aumento de la latencia a las solicitudes de los clientes, debido a la necesidad de recuperar el contenido antes de responder a la solicitud y al aumento del consumo de espacio necesario para los ficheros recuperados del almacenamiento primario.

La lectura de paso a través de FPolicy permite al servidor HSM (el servidor FPolicy) proporcionar acceso de lectura a archivos sin tener que recuperar el archivo del sistema de almacenamiento secundario al sistema de almacenamiento principal. En lugar de recuperar los ficheros de nuevo al almacenamiento primario, las solicitudes de lectura se pueden atender directamente desde un almacenamiento secundario.

> La operación de lectura pasada de FPolicy no admite la descarga de copias (ODX).

La lectura a través de la contraseña mejora la facilidad de uso, ya que proporciona las siguientes ventajas:

- Se pueden atender las solicitudes de lectura incluso si el almacenamiento primario no tiene espacio suficiente para recuperar los datos solicitados de vuelta al almacenamiento primario.
- Mejor gestión de la capacidad y el rendimiento cuando se puede producir un aumento de la recuperación de datos, como si un script o una solución de backup necesitan acceder a numerosos ficheros sin conexión.
- Se pueden atender las solicitudes de lectura de archivos sin conexión en copias snapshot.

  Debido a que las copias Snapshot son de sólo lectura, el servidor FPolicy no puede restaurar el archivo original si el archivo stub se encuentra en una copia snapshot. El uso de la lectura de paso a través elimina este problema.

- Las políticas se pueden configurar para controlar cuándo se atienden las solicitudes de lectura a través del acceso al archivo en el almacenamiento secundario y cuándo debe recuperarse el archivo sin conexión en el almacenamiento primario.

  Por ejemplo, se puede crear una directiva en el servidor HSM que especifique el número de veces que se puede acceder al archivo sin conexión en un periodo de tiempo especificado antes de que se vuelva a migrar al almacenamiento primario. Este tipo de directiva evita recuperar archivos a los que rara vez se accede.

Cómo se gestionan las solicitudes de lectura cuando se habilita la lectura de traspaso de FPolicy

Debe comprender cómo se gestionan las solicitudes de lectura cuando se habilita FPolicy de paso a través de lectura para que pueda configurar de forma óptima la conectividad entre la máquina virtual de almacenamiento (SVM) y los servidores FPolicy.

Cuando la lectura de paso a través de FPolicy está habilitada y la SVM recibe una solicitud de archivo sin conexión, FPolicy envía una notificación al servidor FPolicy (servidor HSM) a través del canal de conexión estándar.

Después de recibir la notificación, el servidor FPolicy lee los datos de la ruta de archivo enviada en la notificación y envía los datos solicitados a la SVM a través de la conexión de datos con privilegios de lectura de paso a paso establecida entre la SVM y el servidor FPolicy.

Una vez enviados los datos, el servidor FPolicy responde a la solicitud de lectura como UN PERMISO o DENEGACIÓN. En función de si se permite o deniega la solicitud de lectura, ONTAP enviará la información

solicitada o enviará un mensaje de error al cliente.