Utilice FPolicy para supervisar y gestionar archivos en SVM

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Utilice FPolicy para supervisar y gestionar archivos en SVM

Comprenda FPolicy

Obtenga más información sobre las soluciones ONTAP 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 de partners incluyen soluciones de terceros 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.

Notificaciones sincrónicas y asincrónicas de ONTAP FPolicy

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 ONTAP FPolicy

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

A partir de ONTAP 9.15.1, se simplifica la configuración de almacén persistente de FPolicy. El `persistent-store create` comando automatiza la creación de volúmenes para la SVM y configura el volumen con prácticas recomendadas de almacenamiento persistente.

Para obtener más información sobre las mejores prácticas de almacén persistente, consulte "Requisitos, consideraciones y prácticas recomendadas para configurar FPolicy".

Para obtener información sobre cómo agregar almacenes persistentes, consulte "Crear almacenes persistentes".

Tipos de configuración de ONTAP 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 archivos que contienen `mp3` extensiones, configure una política para proporcionar notificaciones para determinadas operaciones con extensiones de archivo de destino de `mp3` . La política está configurada para denegar `mp3` solicitudes 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 sobre "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).

Funciones de los componentes del clúster en la implementación de ONTAP 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 ONTAP FPolicy con servidores 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.

Proceso de comunicación de nodo a servidor FPolicy de ONTAP externo

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

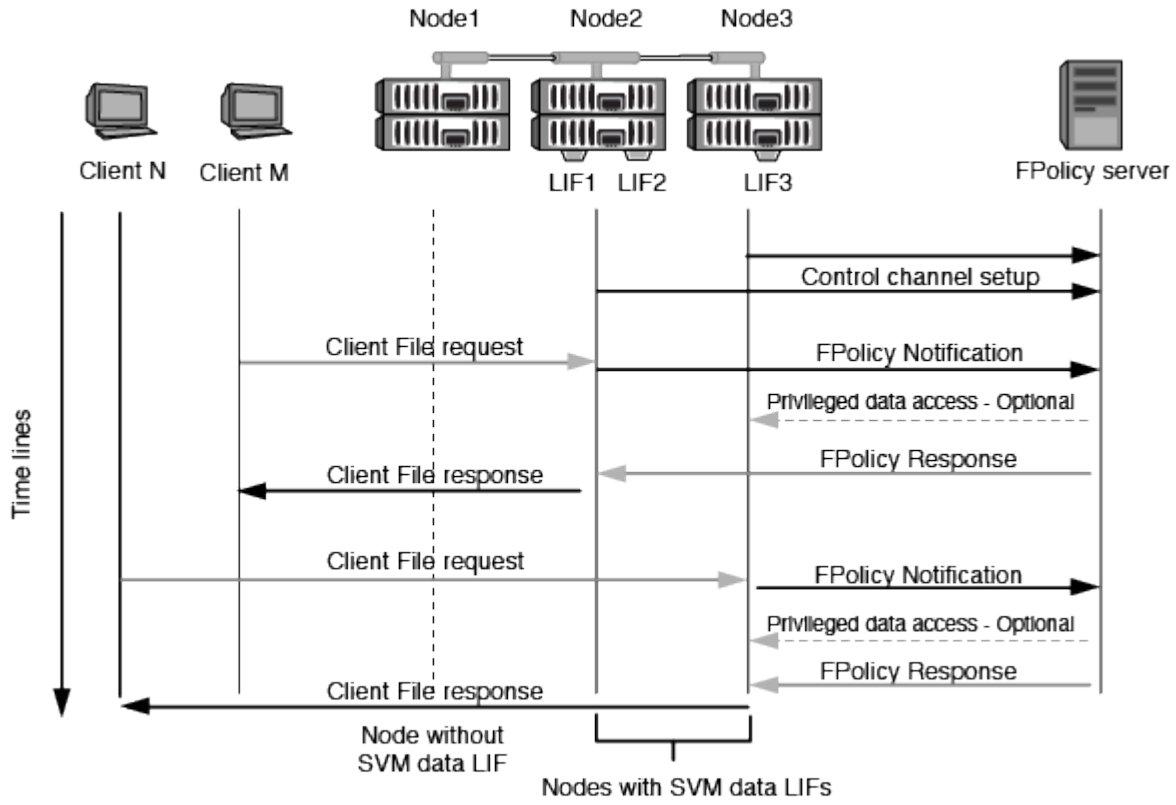
Cada nodo que participa en cada máquina virtual de almacenamiento (SVM) inicia una conexión con un servidor de FPolicy externo (servidor FPolicy) mediante TCP/IP. Las conexiones con los servidores FPolicy se configuran mediante LIF de datos de nodos; por lo tanto, un nodo participante solo puede configurar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

Obtenga información sobre los servicios FPolicy de ONTAP en los espacios de nombres 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 directa de ONTAP FPolicy mejora la usabilidad para la gestión del almacenamiento jerárquico

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.
- Las solicitudes de lectura de archivos sin conexión en instantáneas pueden ser atendidas.

  Dado que las instantáneas son de solo lectura, el servidor FPolicy no puede restaurar el archivo original si el archivo stub está ubicado en una instantánea. 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.

Planifique la configuración de FPolicy

Requisitos, consideraciones y mejores prácticas para configurar ONTAP FPolicy

Antes de crear y configurar las configuraciones de FPolicy en las máquinas virtuales de almacenamiento (SVM), debe tener en cuenta determinados requisitos, consideraciones y prácticas recomendadas para configurar FPolicy.

Las funciones de FPolicy se configuran mediante la interfaz de línea de comandos (CLI) o mediante las API DE REST.

Requisitos para configurar FPolicy

Antes de configurar y habilitar FPolicy en una máquina virtual de almacenamiento (SVM), debe conocer ciertos requisitos.

- Todos los nodos del clúster deben ejecutar una versión de ONTAP que admita FPolicy.
- Si no utiliza el motor de FPolicy nativo de ONTAP, debe tener instalados servidores de FPolicy externos (servidores FPolicy).
- Los servidores de FPolicy deben instalarse en un servidor al que se pueda acceder desde las LIF de datos de la SVM, donde se habilitaron políticas de FPolicy.

> ⓘ A partir de ONTAP 9.8, ONTAP proporciona un servicio LIF de cliente para conexiones FPolicy salientes con la adición `data-fpolicy-client` del servicio. "Más información acerca de los LIF y las políticas de servicio".

- La dirección IP del servidor FPolicy debe configurarse como servidor primario o secundario en la configuración del motor externo de directivas de FPolicy.
- Si los servidores FPolicy acceden a los datos a través de un canal de datos con privilegios, se deben cumplir los siguientes requisitos adicionales:
  - Las licencias de SMB deben estar en el clúster.

    El acceso a datos con privilegios se logra mediante conexiones SMB.
  - Se debe configurar una credencial de usuario para acceder a los archivos a través del canal de datos con privilegios.
  - El servidor FPolicy debe ejecutarse con las credenciales configuradas en la configuración de FPolicy.
  - Todas las LIF de datos utilizadas para comunicarse con los servidores de FPolicy deben configurarse

para que tengan `cifs` uno de los protocolos permitidos.

Esto incluye los LIF utilizados para conexiones de lectura de paso a través.

Prácticas recomendadas y recomendaciones al configurar FPolicy

Cuando configure FPolicy en máquinas virtuales de almacenamiento (SVM), familiarícese con las mejores prácticas y recomendaciones generales de configuración para garantizar que su configuración de FPolicy ofrece un sólido rendimiento de supervisión y resultados que cumplan con sus requisitos.

Para obtener directrices específicas relacionadas con el rendimiento, el ajuste de tamaño y la configuración, utilice su aplicación de partner de FPolicy.

Almacenes persistentes

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.

- Antes de utilizar la funcionalidad de almacén persistente, asegúrese de que sus aplicaciones asociadas admiten esta configuración.
- Se necesita un almacén persistente para cada SVM donde FPolicy esté habilitado.
  - Solo se puede configurar un almacén persistente en cada SVM. Es necesario usar este único almacén persistente para todas las configuraciones de FPolicy en dicho SVM, incluso si las políticas son de partners distintos.
- ONTAP 9.15.1 o posterior:
  - El almacén persistente, su volumen y su configuración de volumen se manejan de forma automática cuando se crea el almacén persistente.
- 9.14.1 de ONTAP:
  - El almacén persistente, su volumen y su configuración de volumen se gestionan de forma manual.
- Cree el volumen de almacenamiento persistente en el nodo con LIF que esperan que FPolicy supervise el tráfico máximo.
  - ONTAP 9.15.1 o posterior: Los volúmenes se crean y configuran automáticamente durante la creación de un almacén persistente.
  - ONTAP 9.14.1: Los administradores del clúster deben crear y configurar un volumen para el almacén persistente en cada una de las SVM donde esté habilitado FPolicy.
- Si las notificaciones acumuladas en el almacén persistente superan el tamaño del volumen aprovisionado, FPolicy iniciará la notificación entrante con los mensajes de EMS adecuados.
  - ONTAP 9.15,1 o posterior: Además del `size` parámetro, el `autosize-mode` parámetro puede ayudar a que el volumen crezca o se reduzca en respuesta a la cantidad de espacio utilizado.
  - ONTAP 9.14,1: `size` El parámetro se configura durante la creación del volumen para que alcance un límite máximo.
- Establezca la política de instantáneas en `none` para el volumen de almacenamiento persistente 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.

    - ONTAP 9.15,1 o posterior: El `snapshot-policy` parámetro se configura automáticamente como ninguno durante la creación del almacén persistente.
    - ONTAP 9.14,1: `snapshot-policy` El parámetro está configurado en `none` durante la creación del volumen.
- 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.
    - ONTAP 9.15.1 o posterior: ONTAP bloquea automáticamente el volumen del acceso al protocolo de usuario externo (CIFS/NFS) durante la creación del almacén persistente.
    - ONTAP 9.14.1: Después de habilitar FPolicy, desmonte el volumen en ONTAP para eliminar la ruta de unión. Esto lo hace inaccesible para el acceso al protocolo de usuario externo (CIFS/NFS).

Para obtener más información, consulte "Almacenes persistentes de FPolicy" y. "Crear almacenes persistentes"

Conmutación al nodo de respaldo y retorno al nodo primario en el almacén persistente

El almacén persistente permanece como estaba 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 almacena y procesa 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 el mismo SVM, las notificaciones que aún no se han procesado también se mueven al nuevo nodo. Necesitas volver a ejecutar el `fpolicy persistent-store create` comando en cualquiera de los nodos después de mover el volumen para garantizar que las notificaciones pendientes se envíen al servidor externo.

Obtenga más información sobre `fpolicy persistent-store create` en el "Referencia de comandos del ONTAP" .

Configuración de directivas

La configuración del motor externo de FPolicy, los eventos y el alcance de SVM pueden mejorar su experiencia y seguridad en general.

- Configuración del motor externo de FPolicy para SVM:
    - Ofrecer seguridad adicional conlleva un coste en el rendimiento. La activación de la comunicación Secure Sockets Layer (SSL) tiene un efecto de rendimiento en el acceso a recursos compartidos.
    - El motor externo de FPolicy debe configurarse con más de un servidor de FPolicy para proporcionar resiliencia y alta disponibilidad del procesamiento de notificaciones de servidor de FPolicy.
- Configuración de eventos de FPolicy para SVM:

  La supervisión de las operaciones de archivos influye en su experiencia general. Por ejemplo, filtrar operaciones de archivos no deseados por el lado del almacenamiento mejora su experiencia. NetApp recomienda configurar la siguiente configuración:

    - Supervisión de los tipos mínimos de operaciones de archivo y activación del número máximo de filtros sin romper el caso de uso.
    - Uso de filtros para operaciones getattr, lectura, escritura, apertura y cierre. Los entornos de directorio

inicial SMB y NFS tienen un alto porcentaje de estas operaciones.

- Configuración del alcance de FPolicy para SVM:

  Restrinja el alcance de las políticas a los objetos de almacenamiento relevantes, como recursos compartidos, volúmenes y exportaciones, en lugar de habilitarlos para toda la SVM. NetApp recomienda comprobar las extensiones del directorio. Si el `is-file-extension-check-on-directories-enabled` parámetro se define en `true`, los objetos de directorio se someten a las mismas comprobaciones de extensiones que los archivos normales.

Configuración de red

La conectividad de red entre el servidor de FPolicy y la controladora debe ser de baja latencia. NetApp recomienda separar el tráfico de FPolicy del tráfico de cliente mediante una red privada.

Además, debe colocar servidores FPolicy externos (servidores de FPolicy) muy cerca del clúster con una conectividad de ancho de banda elevado para proporcionar una latencia mínima y una conectividad de ancho de banda elevado.

> Para una situación en la que el tráfico de LIF para FPolicy está configurado en un puerto diferente a la LIF para el tráfico de cliente, la LIF de FPolicy podría conmutar por error al otro nodo debido a un fallo de puerto. Como resultado, no se puede acceder al servidor FPolicy desde el nodo, lo que provoca que se produzca un error en las notificaciones de FPolicy para las operaciones de archivos en el nodo. Para evitar este problema, compruebe que se pueda acceder al servidor FPolicy a través al menos una LIF del nodo para procesar las solicitudes de FPolicy correspondientes a las operaciones de archivo realizadas en ese nodo.

Configuración de hardware

Puede tener el servidor de FPolicy en un servidor físico o en un servidor virtual. Si el servidor FPolicy se encuentra en un entorno virtual, debe asignar recursos dedicados (CPU, red y memoria) al servidor virtual.

La relación entre el nodo y el servidor FPolicy del clúster debe optimizarse para garantizar que los servidores de FPolicy no estén sobrecargados, lo que puede introducir latencias cuando la SVM responde a las solicitudes de cliente. El ratio óptimo depende de la aplicación asociada para la que se utilice el servidor FPolicy. NetApp recomienda trabajar con partners para determinar el valor adecuado.

Configuración de múltiples políticas

La política de FPolicy para el bloqueo nativo tiene la prioridad más alta, independientemente del número de secuencia, y las políticas que alteran la decisión tienen una prioridad más alta que otras. La prioridad de la política depende del caso de uso. NetApp recomienda trabajar con los partners para determinar la prioridad adecuada.

Consideraciones de tamaño

FPolicy realiza supervisión en línea de las operaciones SMB y NFS, envía notificaciones al servidor externo y espera una respuesta, según el modo de comunicación del motor externo (síncrona o asíncrona). Este proceso afecta al rendimiento del acceso a SMB y NFS y a los recursos de CPU.

Para mitigar cualquier problema, NetApp recomienda trabajar con los partners para evaluar y dimensionar el entorno antes de habilitar FPolicy. El rendimiento se ve afectado por varios factores, como el número de usuarios, las características de la carga de trabajo, como las operaciones por usuario y el tamaño de los datos, la latencia de la red y los fallos o la lentitud del servidor.

Supervisión del rendimiento

FPolicy es un sistema basado en notificaciones. Las notificaciones se envían a un servidor externo para su procesamiento y para generar una respuesta a ONTAP. Este proceso de ida y vuelta aumenta la latencia de acceso de los clientes.

La supervisión de los contadores de rendimiento en el servidor FPolicy y en ONTAP le permite identificar cuellos de botella en la solución y ajustar los parámetros según sea necesario para obtener una solución óptima. Por ejemplo, un aumento de la latencia de FPolicy tiene un efecto en cascada sobre la latencia de acceso de SMB y NFS. Por lo tanto, debería supervisar tanto la latencia de las cargas de trabajo (SMB y NFS) como la latencia de FPolicy. Además, puede utilizar políticas de calidad de servicio en ONTAP para configurar una carga de trabajo para cada volumen o SVM que esté habilitado para FPolicy.

NetApp recomienda ejecutar `statistics show -object workload` el comando para mostrar las estadísticas de carga de trabajo. Además, debe supervisar los siguientes parámetros:

- Latencias medias, de lectura y de escritura
- Número total de operaciones
- Contadores de lectura y escritura

Puede supervisar el rendimiento de los subsistemas de FPolicy utilizando los siguientes contadores de FPolicy.

Debe estar en modo de diagnóstico para recopilar estadísticas relacionadas con FPolicy.

Pasos

1. Recopilar contadores de FPolicy:
   a. `statistics start -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics start -object fpolicy_policy -instance <instance_name> -sample-id <ID>`
2. Mostrar contadores de FPolicy:
   a. `statistics show -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics show -object fpolicy_server -instance <instance_name> -sample-id <ID>`

   Los `fpolicy` `fpolicy_server` contadores y dan información sobre varios parámetros de rendimiento que se describen en la siguiente tabla.

Contadores	Descripción
contadores fpolicy	abortated_requests
Número de solicitudes de pantalla en las que se ha anulado el procesamiento de la máquina virtual de almacenamiento	event_count

Contadores	Descripción
Lista de eventos que generan notificaciones	latencia_solicitud_máx
Latencia máxima de solicitudes de pantalla	outstanding_requests
Número total de solicitudes de pantalla en curso	solicitudes_procesadas
Número total de solicitudes de pantalla que han pasado por el procesamiento de fpolicy en la SVM	hist_latencia_solicitud
Histograma de latencia para solicitudes de pantalla	requests_dispatched_rate
Número de solicitudes de pantalla enviadas por segundo	requests_recepted_rate
Número de solicitudes de pantalla recibidas por segundo	**contadores fpolicy_server**
latencia_solicitud_máx	Latencia máxima para una solicitud de pantalla
outstanding_requests	Número total de solicitudes de pantalla en espera de respuesta
latencia_solicitud	Latencia media para la solicitud de pantalla
hist_latencia_solicitud	Histograma de latencia para solicitudes de pantalla
request_sended_rate	Número de solicitudes de pantalla enviadas al servidor FPolicy por segundo
response_recepted_rate	Número de respuestas de pantalla recibidas del servidor FPolicy por segundo

Obtenga más información sobre `statistics start` y `statistics show` en el "Referencia de comandos del ONTAP".

Gestione el flujo de trabajo de FPolicy y la dependencia de otras tecnologías

NetApp recomienda deshabilitar una política de FPolicy antes de realizar cambios de configuración. Por ejemplo, si desea agregar o modificar una dirección IP en el motor externo configurado para la política activada, desactive primero la política.

Si configura FPolicy para supervisar los volúmenes de NetApp FlexCache, NetApp recomienda que no configure FPolicy para que supervise las operaciones de los archivos de lectura y GETATTR. La supervisión de estas operaciones en ONTAP requiere la recuperación de datos de nodo a ruta (I2P). Dado que no pueden recuperarse datos I2P de volúmenes FlexCache, deben recuperarse del volumen de origen. Por lo tanto, la supervisión de estas operaciones elimina los beneficios de rendimiento que puede ofrecer FlexCache.

Cuando se ponen en marcha FPolicy y una solución antivirus externa, primero la solución antivirus recibe

notificaciones. El procesamiento de FPolicy se inicia solo después de que se complete el análisis antivirus. Es importante dimensionar correctamente las soluciones antivirus porque un análisis antivirus lento puede afectar al rendimiento general.

Consideraciones sobre la actualización de paso a través y la reversión

Hay ciertas consideraciones de actualización y reversión que debe saber acerca de antes de actualizar a una versión ONTAP que admite lectura previa al paso o antes de revertir a una versión que no admite lectura a través del paso.

Actualizar

Después de actualizar todos los nodos a una versión de ONTAP que admita la lectura PassThrough de FPolicy, el clúster puede usar la funcionalidad de lectura mediante paso a paso; sin embargo, la lectura a través permanece deshabilitada de forma predeterminada en las configuraciones de FPolicy existentes. Para utilizar la lectura de paso a través en las configuraciones de FPolicy existentes, debe deshabilitar la política de FPolicy, modificar la configuración y, a continuación, volver a habilitar la configuración.

Revertir

Antes de revertir a una versión de ONTAP que no sea compatible con la lectura de paso a través de FPolicy, debe cumplir las siguientes condiciones:

- Desactive todas las políticas que utilizan passthrough-read y, a continuación, modifique las configuraciones afectadas para que no utilicen passthrough-read.
- Deshabilite la funcionalidad de FPolicy en el clúster deshabilitando todas las políticas de FPolicy en el clúster.

Antes de revertir a una versión de ONTAP que no admite almacenes persistentes, asegúrese de que ninguna de las políticas de FPolicy tenga un almacén persistente configurado. Si se configura un almacén persistente, la reversión fallará.

Información relacionada

- "Las estadísticas muestran"
- "Las estadísticas comienzan"

Configurar las configuraciones de ONTAP FPolicy

Para poder supervisar el acceso a los archivos, debe crearse y habilitarse una configuración de FPolicy en la máquina virtual de almacenamiento (SVM) para la cual se requieren servicios de FPolicy.

Los pasos para configurar y habilitar una configuración de FPolicy en la SVM son los siguientes:

1. Cree un motor externo de FPolicy.

   El motor externo de FPolicy identifica los servidores de FPolicy externos (servidores de FPolicy) asociados con una configuración de FPolicy específica. Si se utiliza el motor de FPolicy interno "'Native'" para crear una configuración nativa de bloqueo de archivos, no será necesario crear un motor externo de FPolicy.

   A partir de ONTAP 9.15,1, puede utilizar `protobuf` el formato del motor. Cuando se establece en `protobuf`, los mensajes de notificación se codifican en formato binario mediante Google Protobuf. Antes de establecer el formato del motor en `protobuf`, asegúrese de que el servidor FPolicy también admite

`protobuf` la deserialización. Para obtener más información, consulte "Planifique la configuración externa del motor de FPolicy"

2. Cree un evento FPolicy.

   Un evento de FPolicy describe lo que debe supervisar la política de FPolicy. Los eventos consisten en los protocolos y las operaciones de archivos que se deben supervisar y pueden contener una lista de filtros. Los eventos utilizan filtros para limitar la lista de eventos supervisados para los que el motor externo de FPolicy debe enviar notificaciones. Los eventos también especifican si la política supervisa las operaciones de volumen.

3. Cree un almacén persistente de FPolicy (opcional).

   A partir de ONTAP 9.14,1, FPolicy permite configurar "almacenes persistentes"para capturar eventos de acceso a archivos para políticas asíncronas no obligatorias en la SVM. No se admiten las configuraciones síncronas (obligatorias o no obligatorias) y asíncronas obligatorias.

   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.

   A partir de ONTAP 9.15.1, se simplifica la configuración de almacén persistente de FPolicy. El `persistent-store-create` comando automatiza la creación de volúmenes para la SVM y configura el volumen para el almacén persistente.

4. Cree una política de FPolicy.

   La directiva FPolicy es responsable de asociar, con el ámbito apropiado, el conjunto de eventos que se deben supervisar y para los que se deben enviar las notificaciones de eventos supervisados al servidor FPolicy designado (o al motor nativo si no hay servidores FPolicy configurados). La directiva también define si se permite al servidor FPolicy el acceso con privilegios a los datos para los que recibe notificaciones. Un servidor FPolicy necesita acceso con privilegios si el servidor necesita acceder a los datos. Entre los casos de uso típicos en los que se necesita un acceso con privilegios se incluyen el bloqueo de archivos, la gestión de cuotas y la gestión del almacenamiento jerárquico. La directiva es donde se especifica si la configuración de esta directiva utiliza un servidor FPolicy o el servidor FPolicy interno "'Native'".

   Una directiva especifica si la selección es obligatoria. Si el tramado es obligatorio y todos los servidores FPolicy están inactivos o no se recibe ninguna respuesta de los servidores FPolicy dentro de un período de tiempo de espera definido, se deniega el acceso al archivo.

   Los límites de una política son la SVM. No es posible aplicar una política a más de una SVM. Sin embargo, una SVM específica puede tener varias políticas de FPolicy, cada una con la misma combinación u otra de configuraciones de alcance, eventos y servidores externos.

5. Configurar el alcance de la directiva.

   El alcance de FPolicy determina qué volúmenes, recursos compartidos o políticas de exportación actúa o se excluye de la supervisión. Un ámbito también determina qué extensiones de archivo se deben incluir o excluir de la supervisión de FPolicy.

   > Las listas de exclusión tienen prioridad sobre las listas de inclusión.

6. Habilite la política de FPolicy.

   Cuando la directiva está activada, se conectan los canales de control y, opcionalmente, los canales de

datos con privilegios. El proceso de FPolicy en los nodos en los que participa la SVM comienza a supervisar el acceso a archivos y carpetas y, en el caso de eventos que coincidan con los criterios configurados, envía notificaciones a los servidores FPolicy (o al motor nativo si no hay servidores FPolicy configurados).

Si la directiva utiliza el bloqueo de archivos nativo, no se configura ni se asocia un motor externo con la directiva.

Planifique la configuración externa del motor de FPolicy

Configuraciones del motor externo de Plan ONTAP FPolicy

Antes de configurar el motor externo de FPolicy, debe comprender qué significa crear un motor externo y qué parámetros de configuración están disponibles. Esta información le ayuda a determinar qué valores se deben establecer para cada parámetro.

Información que se define al crear el motor externo de FPolicy

La configuración del motor externo define la información que FPolicy necesita para realizar y gestionar conexiones con los servidores externos de FPolicy, como lo siguiente:

- Nombre de SVM
- Nombre del motor
- Las direcciones IP de los servidores FPolicy primario y secundario y el número de puerto TCP que se utilizarán al establecer la conexión con los servidores FPolicy
- Si el tipo de motor es asíncrono o síncrono
- Si el formato del motor es `xml` o. `protobuf`

  A partir de ONTAP 9.15,1, puede utilizar `protobuf` el formato del motor. Cuando se establece en `protobuf`, los mensajes de notificación se codifican en formato binario mediante Google Protobuf. Antes de establecer el formato del motor en `protobuf`, asegúrese de que el servidor FPolicy también admite `protobuf` la deserialización.

  Dado que el formato protobuf es compatible a partir de ONTAP 9.15.1, debe considerar el formato de motor externo antes de volver a una versión anterior de ONTAP. Si vuelve a una versión anterior a ONTAP 9.15.1, trabaje con su partner de FPolicy para:

  - Cambie cada formato del motor de `protobuf` a. `xml`
  - Elimine los motores con un formato de motor de `protobuf`
- Cómo autenticar la conexión entre el nodo y el servidor FPolicy

  Si decide configurar la autenticación SSL mutua, también debe configurar parámetros que proporcionen información de certificado SSL.

- Cómo administrar la conexión utilizando varias configuraciones avanzadas de privilegios

  Esto incluye parámetros que definen elementos como valores de tiempo de espera, valores de reintento, valores de mantenimiento activo, valores máximos de solicitud, valores de tamaño de búfer enviados y de recepción y valores de tiempo de espera de sesión.

`vserver fpolicy policy external-engine create`El comando se utiliza para crear un motor externo de FPolicy.

Cuáles son los parámetros básicos del motor externo

Es posible usar la siguiente tabla de parámetros de configuración básicos de FPolicy para ayudar a planificar la configuración:

Tipo de información	Opción
SVM Especifica el nombre de SVM que desea asociar a este motor externo. Cada configuración de FPolicy se define dentro de una única SVM. El motor externo, el evento de políticas, el ámbito de políticas y la política que se combinan para crear una configuración de políticas de FPolicy deben estar todos asociados con la misma SVM.	`-vserver vserver_name`
Nombre del motor Especifica el nombre que se asignará a la configuración externa del motor. Debe especificar el nombre del motor externo más tarde al crear la política de FPolicy. Esto asocia el motor externo a la política. El nombre puede tener hasta 256 caracteres. El nombre debe tener hasta 200 caracteres si se configura el nombre del motor externo en una configuración de recuperación ante desastres de MetroCluster o SVM. El nombre puede contener cualquier combinación de los siguientes caracteres de intervalo ASCII: • `a` a través de `z` • `A` a través de `Z` • `0` a través de `9` • «_», «-`", and ".`»	`-engine-name engine_name`

Servidores principales de FPolicy Especifica los servidores de FPolicy principales a los que el nodo envía notificaciones para una política de FPolicy determinada. El valor se especifica como una lista delimitada por comas de direcciones IP. Si se especifica más de una dirección IP de servidor principal, cada nodo en el que participa la SVM crea una conexión de control a cada servidor de FPolicy principal especificado en el momento en el que se habilita la política. Si configura varios servidores FPolicy principales, las notificaciones se envían a los servidores FPolicy por turnos. Si el motor externo se usa en una configuración de recuperación ante desastres de MetroCluster o SVM, debe especificar las direcciones IP de los servidores FPolicy en el sitio de origen como servidores principales. Las direcciones IP de los servidores FPolicy del sitio de destino se deben especificar como servidores secundarios.	`-primary-servers IP_address,...`
Número de puerto Especifica el número de puerto del servicio FPolicy.	`-port integer`
Servidores secundarios de FPolicy Especifica los servidores de FPolicy secundarios a los que enviar eventos de acceso a archivos para una política de FPolicy determinada. El valor se especifica como una lista delimitada por comas de direcciones IP. Los servidores secundarios sólo se utilizan cuando no se puede acceder a ninguno de los servidores principales. Las conexiones con servidores secundarios se establecen cuando la directiva está habilitada, pero las notificaciones se envían a servidores secundarios sólo si no se puede acceder a ninguno de los servidores principales. Si configura varios servidores secundarios, las notificaciones se envían a los servidores FPolicy por turnos.	`-secondary-servers IP_address,...`
Tipo de motor externo Especifica si el motor externo funciona en modo sincrónico o asíncrono. De forma predeterminada, FPolicy funciona en modo síncrono. Cuando se establece en `synchronous`, el procesamiento de solicitudes de archivo envía una notificación al servidor FPolicy, pero luego no continúa hasta después de recibir una respuesta del servidor FPolicy. En ese punto, el flujo de solicitudes continúa o procesa los resultados en denegación, dependiendo de si la respuesta del servidor FPolicy permite la acción solicitada. Cuando se establece en `asynchronous`, el procesamiento de solicitudes de archivo envía una notificación al servidor FPolicy y, a continuación, continúa.	`-extern-engine-type external_engine_type` El valor de este parámetro puede ser uno de los siguientes: • `synchronous` • `asynchronous`

Formato externo del motor Especifique si el formato de motor externo es xml o protobuf. A partir de ONTAP 9.15.1, puede utilizar el formato de motor protobuf. Cuando se establece en protobuf, los mensajes de notificación se codifican en formato binario utilizando Google Protobuf. Antes de establecer el formato del motor en protobuf, asegúrese de que el servidor FPolicy también admita la deserialización de protobuf.	`- extern-engine-format` {`protobuf` o } `xml`
Opción SSL para la comunicación con el servidor FPolicy Especifica la opción SSL para la comunicación con el servidor FPolicy. Este es un parámetro obligatorio. Puede elegir una de las opciones según la siguiente información: • Cuando se establece en `no-auth`, no se realiza ninguna autenticación. El enlace de comunicación se establece a través de TCP. • Cuando se establece en `server-auth`, la SVM autentica el servidor FPolicy mediante la autenticación de servidor SSL. • Cuando se establece en `mutual-auth`, la autenticación mutua entre el SVM y el servidor FPolicy; el SVM autentica el servidor FPolicy y el servidor FPolicy autentica el SVM. Si decide configurar la autenticación SSL mutua, también debe configurar los `-certificate-common-name` `-certificate -serial` `-certifcate-ca` parámetros , y.	`-ssl-option` {`no-auth`
`server-auth`	`mutual-auth`}
Certificate FQDN o nombre común personalizado Especifica el nombre de certificado utilizado si está configurada la autenticación SSL entre la SVM y el servidor FPolicy. Puede especificar el nombre del certificado como un FQDN o como un nombre común personalizado. Si especifica `mutual-auth` para el `-ssl-option` parámetro, debe especificar un valor para el `-certificate-common-name` parámetro.	`-certificate-common -name` `text`
Número de serie del certificado Especifica el número de serie del certificado utilizado para la autenticación si se configura la autenticación SSL entre la SVM y el servidor FPolicy. Si especifica `mutual-auth` para el `-ssl-option` parámetro, debe especificar un valor para el `-certificate-serial` parámetro.	`-certificate-serial` `text`

Autoridad del certificado Especifica el nombre de CA del certificado utilizado para la autenticación si se configura la autenticación SSL entre la SVM y el servidor FPolicy. Si especifica `mutual-auth` para el `-ssl-option` parámetro, debe especificar un valor para el `-certificate-ca` parámetro.	`-certificate-ca text`

Cuáles son las opciones avanzadas del motor externo

Puede usar la siguiente tabla de parámetros de configuración avanzados de FPolicy conforme planifique si desea personalizar la configuración con parámetros avanzados. Estos parámetros se utilizan para modificar el comportamiento de comunicación entre los nodos del clúster y los servidores FPolicy:

Tipo de información	Opción
Tiempo de espera para cancelar una solicitud Especifica el intervalo de tiempo en horas (`h`), minutos (`m`) o segundos (`s`) que el nodo espera una respuesta del servidor FPolicy. Si el intervalo de tiempo de espera supera, el nodo envía una solicitud de cancelación al servidor FPolicy. A continuación, el nodo envía la notificación a un servidor FPolicy alternativo. Este tiempo de espera ayuda a gestionar un servidor de FPolicy que no responde, lo que puede mejorar la respuesta del cliente SMB/NFS. Además, cancelar las solicitudes después de un período de tiempo de espera puede ayudar a liberar recursos del sistema, ya que la solicitud de notificación se mueve de un servidor FPolicy inactivo/incorrecto a otro servidor FPolicy alternativo. El intervalo de este valor es `0` hasta `100`. Si el valor se establece en `0`, la opción está desactivada y los mensajes de solicitud de cancelación no se envían al servidor FPolicy. El valor predeterminado es `20s`.	`-reqs-cancel-timeout integer`[h
m	s]
Tiempo de espera para cancelar una solicitud Especifica el timeout en horas (`h`), minutos (`m`) o segundos (`s`) para anular una solicitud. El intervalo de este valor es `0` hasta `200`.	`-reqs-abort-timeout ` `integer`[h
m	s]

Intervalo para enviar solicitudes de estado Especifica el intervalo en horas (`h`), minutos (`m`) o segundos (`s`) tras el cual se envía una solicitud de estado al servidor FPolicy. El intervalo de este valor es `0` hasta `50`. Si el valor se establece en `0`, la opción está desactivada y los mensajes de solicitud de estado no se envían al servidor FPolicy. El valor predeterminado es `10s`.	`-status-req-interval integer`[h
m	s]
Número máximo de solicitudes pendientes en el servidor FPolicy Especifica el número máximo de solicitudes pendientes que se pueden poner en cola en el servidor de FPolicy. El intervalo de este valor es `1` hasta `10000`. El valor predeterminado es `500`.	`-max-server-reqs integer`
Timeout para desconectar un servidor de FPolicy que no responde Especifica el intervalo de tiempo en horas (`h`), minutos (`m`) o segundos (`s`) después del cual finaliza la conexión al servidor FPolicy. La conexión finaliza después del período de tiempo de espera sólo si la cola del servidor FPolicy contiene las solicitudes máximas permitidas y no se recibe ninguna respuesta dentro del período de tiempo de espera. El Núm. Máximo permitido de solicitudes es `50` (el valor por defecto) o el Núm. Especificado por el `max-server-reqs-` parámetro. El intervalo de este valor es `1` hasta `100`. El valor predeterminado es `60s`.	`-server-progress -timeout integer`[h
m	s]
Interval para enviar mensajes de mantenimiento activo al servidor de FPolicy Especifica el intervalo de tiempo en horas (`h`), minutos (`m`) o segundos (`s`) en el que se envían mensajes de mantenimiento de la conexión al servidor FPolicy. Los mensajes de mantenimiento activo detectan conexiones medio abiertas. El intervalo de este valor es `10` hasta `600`. Si el valor se establece en `0`, la opción está desactivada y se impide que los mensajes de mantenimiento de conexión se envíen a los servidores FPolicy. El valor predeterminado es `120s`.	`-keep-alive-interval- integer`[h
m	s]

Intentos máximos de reconexión Especifica la cantidad máxima de veces que la SVM intenta volver a conectarse al servidor FPolicy después de haberse roto la conexión. El intervalo de este valor es `0` hasta `20`. El valor predeterminado es `5`.	`-max-connection-retries integer`
Tamaño de búfer de recepción Especifica el tamaño del búfer de recepción del socket conectado para el servidor FPolicy. El valor predeterminado se establece en 256 kilobytes (Kb). Cuando el valor se establece en 0, el tamaño del búfer de recepción se establece en un valor definido por el sistema. Por ejemplo, si el tamaño predeterminado del búfer de recepción del socket es de 65536 bytes, al establecer el valor ajustable en 0, el tamaño del búfer de socket se establece en 65536 bytes. Puede utilizar cualquier valor no predeterminado para establecer el tamaño (en bytes) del búfer de recepción.	`-recv-buffer-size integer`
Tamaño del búfer de envío Especifica el tamaño del búfer de envío del socket conectado para el servidor FPolicy. El valor predeterminado se establece en 256 kilobytes (Kb). Cuando el valor se establece en 0, el tamaño del búfer de envío se establece en un valor definido por el sistema. Por ejemplo, si el tamaño de búfer de envío predeterminado del socket se establece en 65536 bytes, al establecer el valor ajustable en 0, el tamaño del búfer de socket se establece en 65536 bytes. Puede utilizar cualquier valor no predeterminado para establecer el tamaño (en bytes) del búfer de envío.	`-send-buffer-size integer`
Tiempo de espera para purgar un ID de sesión durante la reconexión Especifica el intervalo en horas (`h`), minutos (`m`) o segundos (`s`) tras el cual se envía una nueva Session ID al servidor FPolicy durante los intentos de reconexión. Si la conexión entre la controladora de almacenamiento y el servidor FPolicy se termina y se realiza la reconexión dentro `-session-timeout` del intervalo, la antigua Session ID se envía al servidor FPolicy para que pueda enviar respuestas de las notificaciones anteriores. El valor predefinido se establece en 10 segundos.	`-session-timeout [integerh][integerm][integers]`

Información adicional sobre la configuración de los motores externos de ONTAP FPolicy para utilizar conexiones autenticadas SSL

Debe conocer alguna información adicional si desea configurar el motor externo de FPolicy para usar SSL al conectarse a los servidores de FPolicy.

Autenticación de servidor SSL

Si decide configurar el motor externo de FPolicy para la autenticación del servidor SSL, antes de crear el motor externo, debe instalar el certificado público de la entidad de certificación (CA) que firmó el certificado de servidor FPolicy.

Autenticación mutua

Si configura motores externos de FPolicy para utilizar autenticación mutua de SSL al conectar LIF de datos de máquinas virtuales de almacenamiento (SVM) a servidores FPolicy externos, antes de crear el motor externo, Debe instalar el certificado público de la CA que firmó el certificado de servidor FPolicy junto con el certificado público y el archivo de claves para la autenticación de la SVM. No elimine este certificado mientras ninguna política de FPolicy esté utilizando el certificado instalado.

Si el certificado se elimina mientras FPolicy lo utiliza para autenticación mutua al conectarse a un servidor de FPolicy externo, no podrá volver a habilitar una política de FPolicy deshabilitada que utilice ese certificado. No se puede volver a habilitar la política de FPolicy en esta situación aunque se cree e instale un nuevo certificado con las mismas configuraciones en la SVM.

Si el certificado se ha eliminado, deberá instalar un nuevo certificado, crear nuevos motores externos de FPolicy que utilicen el nuevo certificado y asociar los nuevos motores externos a la política de FPolicy que desee volver a habilitar modificando la directiva de FPolicy.

Instalar certificados para SSL

El certificado público de la CA que se utiliza para firmar el certificado de servidor FPolicy se instala mediante `security certificate install` el comando con el `-type` parámetro establecido en `client-ca`. La clave privada y el certificado público requeridos para la autenticación de la SVM se instala mediante `security certificate install` el comando con `-type` el parámetro establecido en `server`.

Información relacionada

- "instalación del certificado de seguridad"

Los certificados FPolicy de ONTAP no se replican en relaciones de recuperación ante desastres de SVM con una configuración que no preserva la ID

Los certificados de seguridad utilizados para la autenticación SSL al realizar conexiones a servidores FPolicy no replican en destinos de recuperación ante desastres de SVM con configuraciones que no conservan sus ID. Aunque se replica la configuración del motor externo de FPolicy en la SVM, los certificados de seguridad no se replican. Debe instalar manualmente los certificados de seguridad en el destino.

Cuando se configura la relación de recuperación ante desastres de SVM, el valor que se selecciona para `-identity-preserve` la opción `snapmirror create` del comando determina los detalles de configuración que se replican en la SVM de destino.

Si establece `-identity-preserve` la opción en `true` (ID-preserve), se replican todos los detalles de

configuración de FPolicy, incluida la información del certificado de seguridad. Debe instalar los certificados de seguridad en el destino solo si ha establecido la opción en `false` (sin ID-preserve).

Información relacionada

- "snapmirror create"

Restricciones para motores externos de ONTAP FPolicy con ámbito de clúster con configuraciones de recuperación ante desastres de MetroCluster y SVM

Puede crear un motor externo de FPolicy de ámbito de clúster asignando la máquina virtual de almacenamiento (SVM) del clúster al motor externo. Sin embargo, cuando se crea un motor externo de ámbito de clúster en una configuración de recuperación ante desastres de MetroCluster o SVM, existen ciertas restricciones a la hora de elegir el método de autenticación que la SVM utiliza para la comunicación externa con el servidor de FPolicy.

Puede elegir entre tres opciones de autenticación al crear servidores de FPolicy externos: Sin autenticación, autenticación de servidores SSL y autenticación mutua de SSL. Aunque no existen restricciones al elegir la opción de autenticación si se asigna el servidor FPolicy externo a una SVM de datos, al crear un motor externo de FPolicy con ámbito de clúster:

Configuración	¿Permitido?
Recuperación ante desastres de MetroCluster o SVM y un motor externo de FPolicy de ámbito de clúster sin autenticación (SSL no está configurado)	Sí
Recuperación ante desastres de MetroCluster o SVM y un motor externo de FPolicy de ámbito de clúster con servidor SSL o autenticación mutua de SSL	No

- Si existe un motor externo de FPolicy de ámbito de clúster con autenticación SSL y desea crear una configuración de recuperación ante desastres de MetroCluster o SVM, debe modificar este motor externo para que no utilice ninguna autenticación ni quite el motor externo antes de poder crear la configuración de recuperación ante desastres de SVM o MetroCluster.
- Si ya existe la configuración de recuperación ante desastres de MetroCluster o SVM, ONTAP le impide crear un motor externo de FPolicy con ámbito de clúster con autenticación SSL.

Hojas de trabajo completas de configuración del motor externo de ONTAP FPolicy

Puede utilizar esta hoja de trabajo para registrar los valores que necesita durante el proceso de configuración del motor externo de FPolicy. Si es necesario un valor de parámetro, debe determinar qué valor utilizar para esos parámetros antes de configurar el motor externo.

Información para una configuración básica externa del motor

Debe registrar si desea incluir cada parámetro en la configuración externa del motor y, a continuación, registrar el valor de los parámetros que desea incluir.

Tipo de información	Obligatorio	Incluya	Sus valores

El nombre de la máquina virtual de almacenamiento (SVM)	Sí	Sí	
Nombre del motor	Sí	Sí	
Servidores FPolicy principales	Sí	Sí	
Número de puerto	Sí	Sí	
Servidores FPolicy secundarios	No		
Tipo de motor externo	No		
Opción SSL para la comunicación con el servidor FPolicy externo	Sí	Sí	
Nombre común personalizado o FQDN de certificado	No		
Número de serie del certificado	No		
Entidad de certificación	No		

Información para parámetros avanzados del motor externo

Para configurar un motor externo con parámetros avanzados, debe introducir el comando de configuración mientras está en modo de privilegios avanzados.

Tipo de información	Obligatorio	Incluya	Sus valores
Tiempo de espera para cancelar una solicitud	No		
Se ha agotado el tiempo de espera para cancelar una solicitud	No		
Intervalo para enviar solicitudes de estado	No		
Máximo de solicitudes pendientes en el servidor FPolicy	No		
Se ha agotado el tiempo de espera para desconectar un servidor de FPolicy que no responde	No		
Intervalo para enviar mensajes de mantenimiento activo al servidor FPolicy	No		

Número máximo de intentos de reconexión	No		
Tamaño del búfer de recepción	No		
Tamaño del búfer de envío	No		
Se ha agotado el tiempo de espera para purgar un ID de sesión durante la reconexión	No		

Planifique la configuración de eventos de FPolicy

Obtenga más información sobre la configuración del evento de FPolicy de ONTAP

Antes de configurar los eventos de FPolicy, debe comprender lo que significa para crear un evento de FPolicy. Debe determinar qué protocolos desea que se supervise el evento, qué eventos debe supervisar y qué filtros de eventos debe utilizar. Esta información le ayuda a planificar los valores que desea establecer.

Qué significa crear un evento FPolicy

Crear el evento FPolicy significa definir información que el proceso de FPolicy debe determinar qué operaciones de acceso a archivos supervisar y para cuáles de las notificaciones de eventos supervisadas deben enviarse al servidor de FPolicy externo. La configuración del evento FPolicy define la siguiente información de configuración:

- El nombre de la máquina virtual de almacenamiento (SVM)
- Nombre del evento
- Qué protocolos supervisar

  FPolicy puede supervisar operaciones de acceso a archivos SMB, NFSv3, NFSv4 y, a partir de ONTAP 9.15.1, NFSv4,1.

- Qué operaciones de archivos supervisar

  No todas las operaciones de archivo son válidas para cada protocolo.

- Qué archivo se filtra a configurar

  Sólo son válidas determinadas combinaciones de operaciones de archivos y filtros. Cada protocolo tiene su propio conjunto de combinaciones compatibles.

- Si se supervisan las operaciones de montaje y desmontaje de volúmenes

Hay una dependencia con tres de los parámetros (`-protocol`, , `-file-operations -filters`). Las siguientes combinaciones son válidas para los tres parámetros:

- Puede especificar los `-protocol` `-file-operations` parámetros y.
- Es posible especificar los tres parámetros.
- No es posible especificar ninguno de los parámetros.

Lo que contiene la configuración del evento FPolicy

Es posible usar la siguiente lista de parámetros de configuración de eventos de FPolicy disponibles para ayudar a planificar la configuración:

Tipo de información	Opción
SVM Especifica el nombre de la SVM que desea asociar a este evento de FPolicy. Cada configuración de FPolicy se define dentro de una única SVM. El motor externo, el evento de políticas, el ámbito de políticas y la política que se combinan para crear una configuración de políticas de FPolicy deben estar todos asociados con la misma SVM.	`-vserver` `vserver_name`
Nombre del evento Especifica el nombre que se asignará al evento FPolicy. Cuando crea la política de FPolicy, debe asociar el evento FPolicy con la política mediante el nombre del evento. El nombre puede tener hasta 256 caracteres. El nombre debe tener hasta 200 caracteres si configura el evento en una configuración de recuperación ante desastres de MetroCluster o SVM. El nombre puede contener cualquier combinación de los siguientes caracteres de intervalo ASCII: • `a` a través de `z` • `A` a través de `Z` • `0` a través de `9` • “ _,“`-`", and ".`””	`-event-name` `event_name`

Protocolo Especifica el protocolo que se configurará para el evento FPolicy. La lista de `-protocol` puede incluir uno de los siguientes valores: • `cifs` • `nfsv3` • `nfsv4` Si especifica `-protocol`, debe especificar un valor válido en el `-file-operations` parámetro. A medida que cambie la versión del protocolo, es posible que los valores válidos cambien. A partir de ONTAP 9.15.1, NFSv4 le permite capturar eventos NFSv4,0 y NFSv4,1.	`-protocol protocol`

Operaciones de archivo Especifica la lista de operaciones de archivo para el evento FPolicy. El evento comprueba las operaciones especificadas en esta lista de todas las solicitudes de cliente que utilizan el protocolo especificado en el `-protocol` parámetro. Puede enumerar una o varias operaciones de archivo usando una lista delimitada por comas. La lista de `-file-operations` puede incluir uno o más de los siguientes valores: • `close` en el caso de operaciones de cierre de archivos • `create` para operaciones de creación de archivos • `create-dir` para las operaciones de creación de directorios • `delete` para operaciones de eliminación de archivos • `delete_dir` para operaciones de eliminación de directorios • `getattr` para las operaciones de obtención de atributos • `link` para operaciones de enlace • `lookup` para operaciones de consulta • `open` para operaciones de apertura de archivos • `read` para operaciones de lectura de archivos • `write` para operaciones de escritura de archivos • `rename` para operaciones de cambio de nombre de archivos • `rename_dir` para operaciones de cambio de nombre de directorios • `setattr` para operaciones de definición de atributos • `symlink` para operaciones de enlace simbólico Si especifica `-file-operations`, debe especificar un protocolo válido en el `-protocol` parámetro.	`-file-operations file_operations,...`

Filtros Especifica la lista de filtros para una operación de archivo determinada para el protocolo especificado. Los valores del `-filters` parámetro se utilizan para filtrar solicitudes de cliente. La lista puede incluir una o varias de las siguientes opciones: Si especifica `-filters` el parámetro, también debe especificar valores válidos para los `-file-operations -protocol` parámetros y. • `monitor-ads` opción para filtrar la solicitud de cliente para un flujo de datos alternativo. • `close-with-modification` opción para filtrar la solicitud de cliente para cerrar con modificación. • `close-without-modification` opción para filtrar la solicitud del cliente para cerrar sin modificación. • `first-read` opción para filtrar la solicitud de cliente para la primera lectura. • `first-write` opción de filtrar la solicitud del cliente para la primera escritura. • `offline-bit` opción para filtrar la solicitud del cliente para el juego de bits fuera de línea. Al establecer este filtro, el servidor FPolicy recibe una notificación solo cuando se accede a los archivos sin conexión. • `open-with-delete-intent` opción para filtrar la solicitud de cliente para abierta con intención de supresión. Al establecer este filtro, el servidor FPolicy recibe la notificación sólo cuando se intenta abrir un archivo con la intención de eliminarlo. Esto lo utilizan los sistemas de archivos cuando `FILE_DELETE_ON_CLOSE` se especifica el indicador. • `open-with-write-intent` opción para filtrar la solicitud de cliente para abierta con intención de escritura. Al establecer este filtro, el servidor FPolicy recibe la notificación sólo cuando se intenta abrir un archivo con la intención de escribir algo en él. • `write-with-size-change` opción de filtrar la solicitud de cliente de escritura con cambio de tamaño. • `setattr-with-owner-change` opción para filtrar las solicitudes de setattr del cliente para cambiar el propietario de un archivo o un directorio. • `setattr-with-group-change` opción para filtrar las solicitudes de setattr del cliente para cambiar el grupo de un archivo o un directorio. • `setattr-with-sacl-change` Opción para filtrar las solicitudes de setattr del cliente para cambiar el SACL en un archivo o directorio.	`-filters filter, ...`

32 Este filtro solo está disponible para los protocolos SMB y NFSv4.

Is operación de volumen requerida Especifica si se requiere la supervisión para las operaciones de montaje y desmontaje de volúmenes. El valor predeterminado es `false`.	`-volume-operation {true`

`false}`
 	
`-filters filter, ...`
	Notificaciones denegadas de acceso a FPolicy
	
	A partir de ONTAP 9.13.1, los usuarios pueden recibir notificaciones por operaciones de archivos fallidas debido a la falta de permisos. Estas notificaciones son valiosas para la seguridad, la protección contra el ransomware y la gobernanza. Se generarán notificaciones para la operación de archivo fallida debido a la falta de permiso, que incluye:
	
	• Fallos debidos a permisos NTFS.
	• Fallos debidos a bits de modo Unix.
	• Fallos debidos a NFSv4 ACL.

`-monitor-fileop-failure {true` Cuando se especifica este filtro, las operaciones de directorio no se supervisan.	`false}`

Combinaciones de filtros y operaciones de archivos compatibles que ONTAP FPolicy supervisa para SMB

Al configurar el evento de FPolicy, debe tener en cuenta que solo ciertas combinaciones de operaciones y filtros de archivos son compatibles para supervisar las operaciones de acceso a archivos SMB.

La lista de operaciones de archivos y combinaciones de filtros admitidas para la supervisión de FPolicy de los eventos de acceso a archivos SMB se proporciona en la siguiente tabla:

Operaciones de archivos admitidas	Filtros compatibles
cierre	anuncios de monitor, bit sin conexión, primer plano con modificación, primer plano sin modificación, primer plano con lectura, excluir directorio
cree	anuncios de monitores, bits sin conexión
create_dir	Actualmente no hay ningún filtro compatible con esta operación de archivo.

eliminar	anuncios de monitores, bits sin conexión
delete_dir	Actualmente no hay ningún filtro compatible con esta operación de archivo.
getattr	bit sin conexión, exclude-dir
abierto	anuncios de monitores, bits sin conexión, intento de borrado, intento de escritura abierta, dir de exclusión
lea	anuncios de monitores, bits sin conexión, primera lectura
escritura	anuncios de monitor, bits sin conexión, primera escritura, escritura con cambio de tamaño
cambiar el nombre	anuncios de monitores, bits sin conexión
dir_renombrar	Actualmente no hay ningún filtro compatible con esta operación de archivo.
setattr	anuncios de monitor, offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_time_change, setattr_with_size_change, setattr_with_asition_size_change, exclude_directory

A partir de ONTAP 9.13.1, los usuarios pueden recibir notificaciones por operaciones de archivos fallidas debido a la falta de permisos. En la siguiente tabla se proporciona la lista de combinaciones de acceso admitido denegado y filtros para la supervisión de FPolicy de los eventos de acceso a archivos SMB:

Se admite la operación de archivo denegado de acceso	Filtros compatibles
abierto	NA

Combinaciones de filtros y operaciones de archivos compatibles que ONTAP FPolicy monitorea para NFSv3

Cuando configura su evento de FPolicy, debe tener en cuenta que solo ciertas combinaciones de operaciones y filtros son compatibles para supervisar las operaciones de acceso a archivos NFSv3.

La lista de operaciones de archivos y combinaciones de filtros admitidas para la supervisión de FPolicy de los eventos de acceso a archivos NFSv3 se proporciona en la siguiente tabla:

Operaciones de archivos admitidas	Filtros compatibles

cree	bit sin conexión
create_dir	Actualmente no hay ningún filtro compatible con esta operación de archivo.
eliminar	bit sin conexión
delete_dir	Actualmente no hay ningún filtro compatible con esta operación de archivo.
enlace	bit sin conexión
búsqueda	bit sin conexión, exclude-dir
lea	bit sin conexión, primera lectura
escritura	sin conexión-bit, primera escritura, escritura-con-cambio de tamaño
cambiar el nombre	bit sin conexión
dir_renombrar	Actualmente no hay ningún filtro compatible con esta operación de archivo.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
enlace simbólico	bit sin conexión

A partir de ONTAP 9.13.1, los usuarios pueden recibir notificaciones por operaciones de archivos fallidas debido a la falta de permisos. En la siguiente tabla se proporciona la lista de combinaciones de acceso admitido denegado y filtros para la supervisión de FPolicy de eventos de acceso a archivos NFSv3:

Se admite la operación de archivo denegado de acceso	Filtros compatibles
acceso	NA
cree	NA
create_dir	NA
eliminar	NA
delete_dir	NA
enlace	NA

lea	NA
cambiar el nombre	NA
dir_renombrar	NA
setattr	NA
escritura	NA

Combinaciones de filtros y operaciones de archivos compatibles que ONTAP FPolicy monitorea para NFSv4

Cuando configura su evento de FPolicy, debe tener en cuenta que solo ciertas combinaciones de operaciones y filtros son compatibles para supervisar las operaciones de acceso a archivos NFSv4.

A partir de ONTAP 9.15.1, FPolicy admite el protocolo NFSv4,1.

En la siguiente tabla se proporciona la lista de combinaciones de operaciones de archivos y filtros admitidas para la supervisión de FPolicy de los eventos de acceso a archivos NFSv4 o NFSv4,1:

Operaciones de archivos admitidas	Filtros compatibles
cierre	fuera de línea, directorio de exclusión
cree	bit sin conexión
create_dir	Actualmente no hay ningún filtro compatible con esta operación de archivo.
eliminar	bit sin conexión
delete_dir	Actualmente no hay ningún filtro compatible con esta operación de archivo.
getattr	fuera de línea, directorio de exclusión
enlace	bit sin conexión
búsqueda	fuera de línea, directorio de exclusión
abierto	fuera de línea, directorio de exclusión
lea	bit sin conexión, primera lectura
escritura	sin conexión-bit, primera escritura, escritura-con-cambio de tamaño

cambiar el nombre	bit sin conexión
dir_renombrar	Actualmente no hay ningún filtro compatible con esta operación de archivo.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
enlace simbólico	bit sin conexión

A partir de ONTAP 9.13.1, los usuarios pueden recibir notificaciones por operaciones de archivos fallidas debido a la falta de permisos. En la siguiente tabla se proporciona la lista de combinaciones de acceso admitido denegado y filtros para la supervisión de FPolicy de eventos de acceso a archivos NFSv4 o NFSv4,1:

Se admite la operación de archivo denegado de acceso	Filtros compatibles
acceso	NA
cree	NA
create_dir	NA
eliminar	NA
delete_dir	NA
enlace	NA
abierto	NA
lea	NA
cambiar el nombre	NA
dir_renombrar	NA
setattr	NA
escritura	NA

Hojas de trabajo completas de configuración de eventos de ONTAP FPolicy

Puede utilizar esta hoja de datos para registrar los valores que necesita durante el

proceso de configuración de eventos de FPolicy. Si un valor de parámetro es obligatorio, debe determinar qué valor se debe usar para esos parámetros antes de configurar el evento FPolicy.

Debe registrar si desea incluir cada ajuste de parámetros en la configuración de eventos de FPolicy y, a continuación, registrar el valor para los parámetros que desea incluir.

Tipo de información	Obligatorio	Incluya	Sus valores
El nombre de la máquina virtual de almacenamiento (SVM)	Sí	Sí	
Nombre del evento	Sí	Sí	
Protocolo	No		
Operaciones de archivos	No		
Filtros	No		
Operación de volumen	No		
Acceso denegado a eventos + (soporte a partir de ONTAP 9,13)	No		

Planifique la configuración de la política de FPolicy

Obtenga más información sobre las configuraciones de políticas de ONTAP FPolicy

Antes de configurar la política de FPolicy, debe comprender qué parámetros son necesarios para crear la política y por qué quizás desee configurar determinados parámetros opcionales. Esta información le ayuda a determinar qué valores se deben establecer para cada parámetro.

Al crear una política de FPolicy, debe asociar la política a lo siguiente:

- La máquina virtual de almacenamiento (SVM)
- Uno o más eventos de FPolicy
- Un motor externo de FPolicy

También puede configurar varias opciones de configuración de directivas.

Lo que contiene la configuración de la política de FPolicy

Puede usar la siguiente lista de políticas de FPolicy disponibles y parámetros opcionales para ayudar a planificar la configuración:

Tipo de información	Opción	Obligatorio	Predeterminado

SVM name Especifica el nombre de la SVM en la que desea crear una política de FPolicy.	`-vserver vserver_name`	Sí	Ninguno
Nombre de directiva Especifica el nombre de la política de FPolicy. El nombre puede tener hasta 256 caracteres. El nombre debe tener hasta 200 caracteres si se configura la política en una configuración de recuperación ante desastres de MetroCluster o SVM. El nombre puede contener cualquier combinación de los siguientes caracteres de intervalo ASCII: • `a` a través de `z` • `A` a través de `Z` • `0` a través de `9` • «_», «-`", and ".`»	`-policy-name policy_name`	Sí	Ninguno
Nombres de eventos Especifica una lista de eventos delimitada por comas para asociarlos a la directiva de FPolicy. • Puede asociar más de un evento a una directiva. • Un evento es específico de un protocolo. • Puede utilizar una única directiva para supervisar los eventos de acceso a archivos de más de un protocolo creando un evento para cada protocolo que desee supervisar la directiva y asociando los eventos a la directiva. • Los eventos deben existir previamente.	`-events event_name, ...`	Sí	Ninguno

Almacén persistente A partir de ONTAP 9.14.1, este parámetro especifica el almacén persistente para capturar eventos de acceso a archivos para políticas asíncronas no obligatorias en la SVM.	`-persistent -store persistent_store_name`	No	Ninguno
Nombre externo del motor Especifica el nombre del motor externo que se va a asociar a la directiva de FPolicy. • Un motor externo contiene información que el nodo necesita para enviar notificaciones a un servidor FPolicy. • Es posible configurar FPolicy para usar el motor externo nativo de ONTAP para bloquear archivos fácilmente o para usar un motor externo que esté configurado para utilizar servidores de FPolicy externos (servidores FPolicy) a fin de ofrecer un bloqueo de archivos y una gestión de archivos más sofisticados. • Si desea utilizar el motor externo nativo, no puede especificar un valor para este parámetro o puede especificarlo como `native` valor. • Si desea utilizar servidores FPolicy, la configuración del motor externo ya debe existir.	`-engine engine_name`	Sí (a menos que la política utilice el motor nativo de ONTAP interno)	`native`

Es obligatoria la selección requerida Especifica si es necesario realizar un análisis de acceso a archivos obligatorio. • La configuración de tramado obligatoria determina qué acción se realiza en un evento de acceso a archivos en un caso en que todos los servidores principales y secundarios están inactivos o no se recibe respuesta de los servidores FPolicy dentro de un período de tiempo de espera determinado. • Cuando se define en `true`, se rechazan los eventos de acceso a archivos. • Cuando se define en `false`, se permiten eventos de acceso a archivos.	`-is-mandatory {true`	`false}`	No

`true`	*Permitir acceso privilegiado* Especifica si desea que el servidor FPolicy tenga acceso privilegiado a los archivos y carpetas supervisados mediante una conexión de datos con privilegios. Si se configura, los servidores FPolicy pueden acceder a archivos desde la raíz de la SVM que contiene los datos supervisados mediante la conexión de datos con privilegios. Para acceder a los datos con privilegios, se debe tener una licencia de SMB en el clúster y todas las LIF de datos utilizadas para conectarse a los servidores de FPolicy se deben configurar para que tengan `cifs` como uno de los protocolos permitidos. Si desea configurar la directiva para permitir el acceso con privilegios, también debe especificar el nombre de usuario de la cuenta que desea que el servidor FPolicy utilice para obtener acceso con privilegios.	`-allow -privileged -access {yes`	`no}`

No (a menos que la lectura directa esté habilitada)	`no`	*Nombre de usuario privilegiado* Especifica el nombre de usuario de la cuenta que utilizan los servidores FPolicy para el acceso a datos con privilegios. • El valor de este parámetro debe utilizar el formato "dain\user name". • Si `-allow -privileged -access` se establece en `no`, se ignorará cualquier valor establecido para este parámetro.	`-privileged -user-name user_name`

No (a menos que el acceso con privilegios esté activado)	Ninguno	*Permitir passThrough-read* Especifica si los servidores FPolicy pueden proporcionar servicios de lectura de paso a través para los archivos que los servidores FPolicy han archivado en almacenamiento secundario (archivos sin conexión): • La lectura mediante paso es una forma de leer datos de archivos sin conexión sin restaurar los datos en el almacenamiento primario. La lectura tras paso reduce las latencias de respuesta, ya que no es necesario recuperar los archivos en el almacenamiento principal antes de responder a la solicitud de lectura. Además, la lectura tras paso optimiza la eficiencia del almacenamiento , ya que elimina la necesidad de consumir espacio de almacenamiento primario con archivos que se recuperan únicamente para satisfacer las solicitudes de lectura. Cuando se	`-is-passthrough -read-enabled {true`

Requisito para las configuraciones del alcance de FPolicy de ONTAP si la política de FPolicy utiliza el motor nativo

Si configura la política de FPolicy para utilizar el motor nativo, hay un requisito específico para definir el ámbito de FPolicy configurado para la política.

El alcance de FPolicy define los límites en los que se aplica la política de FPolicy, por ejemplo, si se aplica a volúmenes o recursos compartidos especificados. Hay una serie de parámetros de ámbito al que se aplica la política de FPolicy. Uno de estos parámetros es `-is-file-extension-check-on-directories-enabled`, , especifica si se deben comprobar las extensiones de archivo en los directorios. El valor por defecto es `false`, lo que significa que no se comprueban las extensiones de archivo de los directorios.

Cuando se habilita una política de FPolicy que utiliza el motor nativo en un recurso compartido o volumen y el `-is-file-extension-check-on-directories-enabled` parámetro se establece en `false` para el ámbito de la política, se deniega el acceso a directorios. Con esta configuración, dado que las extensiones de archivo no se comprueban en busca de directorios, cualquier operación de directorio se deniega si está dentro del ámbito de la directiva.

Para garantizar que el acceso al directorio se realice correctamente al utilizar el motor nativo, debe definir el `-is-file-extension-check-on-directories-enabled parameter` en `true` al crear el ámbito.

Con este parámetro definido en `true`, se realizan comprobaciones de extensión para las operaciones de directorio y la decisión de permitir o denegar el acceso se toma en función de las extensiones incluidas o excluidas en la configuración de ámbito de FPolicy.

- Habilita, los servidores FPolicy proporcionan los datos para el archivo a través de un canal de datos privilegiado independiente.
- `-is-file-extension-check-on-directories-enabled` especifica si se deben comprobar las extensiones de archivo en los directorios.
- Si desea configurar passthrough-read, la directiva también debe configurarse para permitir el acceso privilegiado.

Hojas de trabajo completas de políticas de ONTAP FPolicy

Puede utilizar esta hoja de trabajo para registrar los valores que necesita durante el proceso de configuración de directivas de FPolicy. Debe registrar si desea incluir cada configuración de parámetros en la configuración de políticas de FPolicy y, a continuación, registrar el valor para los parámetros que desea incluir.

Tipo de información	Incluya	Sus valores
El nombre de la máquina virtual de almacenamiento (SVM)	Sí	
Nombre de la política	Sí	
Nombres de eventos	Sí	
Almacenamiento persistente		
Nombre del motor externo		
¿Es obligatorio realizar pruebas de detección?		
Permitir acceso privilegiado		

Nombre de usuario privilegiado		
¿Está habilitada la lectura PassThrough?		

Planifique la configuración del alcance de FPolicy

Obtenga más información sobre las configuraciones del alcance de ONTAP FPolicy

Antes de configurar el ámbito de FPolicy, debe comprender qué significa para crear un ámbito. Debe comprender qué contiene la configuración del ámbito. También debe comprender cuáles son las reglas de alcance de prioridad. Esta información puede ayudarle a planificar los valores que desea establecer.

Qué significa crear un alcance de FPolicy

Crear el ámbito de FPolicy significa definir los límites en los que se aplica la política de FPolicy. La máquina virtual de almacenamiento (SVM) es el límite básico. Cuando se crea un alcance para una política de FPolicy, debe definir la política de FPolicy a la que se aplicará y debe designar a las SVM que desee aplicar el alcance.

Hay una serie de parámetros que restringen aún más el ámbito dentro de la SVM especificada. Puede restringir el ámbito especificando qué incluir en el ámbito o especificando qué excluir del ámbito. Después de aplicar un ámbito a una política habilitada, las comprobaciones de eventos de política se aplican al ámbito definido por este comando.

Se generan notificaciones para eventos de acceso a archivos en los que se encuentran coincidencias en las opciones de «incluir». No se generan notificaciones para eventos de acceso a archivos en los que se encuentran coincidencias en las opciones "'exclude'".

La configuración del alcance de FPolicy define la siguiente información de configuración:

- Nombre de SVM
- Nombre de la política
- Los recursos compartidos que se van a incluir o excluir de lo que se supervisa
- Las políticas de exportación que se van a incluir o excluir de lo que se supervise
- Los volúmenes que se van a incluir o excluir de lo que se supervise
- Extensiones de archivo que se van a incluir o excluir de lo que se supervisa
- Si se realizan comprobaciones de extensión de archivo en objetos de directorio

> Existen consideraciones especiales para el ámbito de una política de FPolicy de clúster. La política de FPolicy del clúster es una política que el administrador de clúster crea para la SVM de administrador. Si el administrador de clúster también crea el ámbito para esa política de FPolicy de clúster, el administrador de SVM no puede crear un ámbito para esa misma política. Sin embargo, si el administrador de clúster no crea un ámbito para la política de FPolicy de clúster, todos los administradores de SVM pueden crear el ámbito para esa política de clúster. Si el administrador de SVM crea un ámbito para esa política de FPolicy de clúster, el administrador de clúster no podrá crear posteriormente un alcance de clúster para esa misma política de clúster. Esto se debe a que el administrador de clúster no puede anular el ámbito de la misma política de clúster.

Cuáles son las reglas de alcance de prioridad

Las siguientes reglas de prioridad se aplican a las configuraciones del ámbito:

- Cuando se incluye un recurso compartido en el `-shares-to-include` parámetro y el volumen principal del recurso compartido se incluye en el `-volumes-to-exclude` parámetro, `-volumes-to-exclude` tiene prioridad sobre `-shares-to-include`.
- Cuando se incluye una política de exportación en `-export-policies-to-include` el parámetro y el volumen primario de la política de exportación se incluye en `-volumes-to-exclude` el parámetro, `-volumes-to-exclude` tiene prioridad sobre `-export-policies-to-include`.
- Un administrador puede especificar `-file-extensions-to-include` `-file-extensions-to-exclude` listas y.

  El `-file-extensions-to-exclude` parámetro se comprueba antes de `-file-extensions-to-include` comprobar el parámetro.

Lo que contiene la configuración del alcance de FPolicy

Es posible usar la siguiente lista de parámetros de configuración del ámbito de FPolicy disponibles para ayudar a planificar la configuración:

> Al configurar qué recursos compartidos, políticas de exportación, volúmenes y extensiones de archivos para incluir o excluir del ámbito, los parámetros de inclusión y exclusión pueden incluir metacaracteres como "`?` and `*`". No se admite el uso de expresiones regulares.

Tipo de información	Opción
SVM Especifica el nombre de la SVM donde desea crear un alcance de FPolicy. Cada configuración de FPolicy se define dentro de una única SVM. El motor externo, el evento de políticas, el ámbito de políticas y la política que se combinan para crear una configuración de políticas de FPolicy deben estar todos asociados con la misma SVM.	`-vserver vserver_name`
Nombre de directiva Especifica el nombre de la política de FPolicy a la que desea asociar el ámbito. Debe haber la política de FPolicy.	`-policy-name policy_name`
Acciones a incluir Especifica una lista de recursos compartidos delimitados por comas que se van a supervisar la política de FPolicy a la que se aplica el ámbito.	`-shares-to-include share_name, ...`

Acciones para excluir Especifica una lista de recursos compartidos delimitados por comas que se van a excluir de la supervisión de la política de FPolicy a la que se aplica el ámbito.	`-shares-to-exclude share_name, ...`
Volumes to include especifica una lista de volúmenes delimitada por comas que supervisar la política de FPolicy a la que se aplica el ámbito.	`-volumes-to-include volume_name, ...`
Volúmenes para excluir Especifica una lista delimitada por comas de volúmenes que se van a excluir de la supervisión de la política de FPolicy a la que se aplica el ámbito.	`-volumes-to-exclude volume_name, ...`
Export Policies to include Especifica una lista delimitada por comas de políticas de exportación que se deben supervisar para la directiva de FPolicy a la que se aplica el ámbito.	`-export-policies-to -include export_policy_name, ...`
Exportar directivas para excluir Especifica una lista delimitada por comas de políticas de exportación que se van a excluir de la supervisión de la directiva de FPolicy a la que se aplica el ámbito.	`-export-policies-to -exclude export_policy_name, ...`
Extensiones de archivo para incluir Especifica una lista delimitada por comas de extensiones de archivo que se va a supervisar para la directiva de FPolicy a la que se aplica el ámbito.	`-file-extensions-to -include file_extensions, ...`
Extensión de archivo para excluir Especifica una lista delimitada por comas de extensiones de archivo que se van a excluir de la supervisión de la directiva de FPolicy a la que se aplica el ámbito.	`-file-extensions-to -exclude file_extensions, ...`
Es la comprobación de la extensión del archivo en el directorio activado ? Especifica si las comprobaciones de extensión de nombre de archivo también se aplican a los objetos de directorio. Si este parámetro se define en `true`, los objetos de directorio se someten a las mismas comprobaciones de extensiones que los archivos normales. Si este parámetro está definido en `false`, los nombres de directorio no coinciden con las extensiones y se envían notificaciones para los directorios aunque sus extensiones de nombre no coincidan. Si la política de FPolicy a la que se asigna el ámbito está configurada para utilizar el motor nativo, este parámetro se debe establecer en `true`.	`-is-file-extension -check-on-directories -enabled{true false`
	}

Hojas de trabajo completas del alcance de la política de ONTAP

Esta hoja de trabajo se puede usar para registrar los valores necesarios durante el proceso de configuración del ámbito de FPolicy. Si es necesario un valor de parámetro, debe determinar qué valor se debe usar para esos parámetros antes de configurar el alcance de FPolicy.

Debe registrar si desea incluir cada configuración de parámetros en la configuración del ámbito de FPolicy y, a continuación, registrar el valor para los parámetros que desea incluir.

Tipo de información	Obligatorio	Incluya	Sus valores
El nombre de la máquina virtual de almacenamiento (SVM)	Sí	Sí	
Nombre de la política	Sí	Sí	
Recursos compartidos que incluir	No		
Recursos compartidos para excluir	No		
Volúmenes que incluir	No		
Volúmenes para excluir	No		
Las políticas de exportación que se incluirán	No		
Directivas de exportación para excluir	No		
Extensiones de archivo que se incluirán	No		
Extensión de archivo para excluir	No		
¿Está activada la comprobación de extensión de archivo en el directorio?	No		

Cree la configuración de FPolicy

Crear motores externos de ONTAP FPolicy

Debe crear un motor externo para comenzar a crear una configuración de FPolicy. El motor externo define el modo en que FPolicy realiza y gestiona conexiones a servidores FPolicy externos. Si su configuración utiliza el motor interno de ONTAP (el motor externo nativo) para bloquear archivos de forma sencilla, no tendrá que configurar un motor externo de FPolicy independiente y no tenga que llevar a cabo este paso.

Antes de empezar

La "motor externo" hoja de trabajo debe completarse.

Acerca de esta tarea

Si el motor externo se utiliza en una configuración de MetroCluster, debe especificar las direcciones IP de los servidores FPolicy del sitio de origen como servidores principales. Las direcciones IP de los servidores FPolicy del sitio de destino se deben especificar como servidores secundarios.

Pasos

1. Cree el motor externo de FPolicy mediante `vserver fpolicy policy external-engine create` el comando.

   El siguiente comando crea un motor externo en una máquina virtual de almacenamiento (SVM) vs1.example.com. No se requiere autenticación para las comunicaciones externas con el servidor FPolicy.

   ```
   vserver fpolicy policy external-engine create -vserver-name vs1.example.com
   -engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
   no-auth
   ```

2. Compruebe la configuración del motor externo de FPolicy mediante `vserver fpolicy policy external-engine show` el comando.

   El siguiente comando muestra información acerca de todos los motores externos configurados en SVM vs1.example.com:

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com
   ```

   ```
                                Primary        Secondary
   External
   Vserver             Engine       Servers        Servers       Port Engine
   Type
   ---------------     -----------  -------------- ----------- ------
   -----------
   vs1.example.com     engine1      10.1.1.2,      -             6789
   synchronous
                                    10.1.1.3
   ```

   El siguiente comando muestra información detallada sobre el motor externo denominado «'motor1'» en la SVM vs1.example.com:

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
   -name engine1
   ```

```
                            Vserver: vs1.example.com
                             Engine: engine1
              Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
       Port Number of FPolicy Service: 6789
            Secondary FPolicy Servers: -
                 External Engine Type: synchronous
SSL Option for External Communication: no-auth
           FQDN or Custom Common Name: -
         Serial Number of Certificate: -
               Certificate Authority: -
```

Crear eventos de ONTAP FPolicy

Como parte de la creación de una configuración de políticas de FPolicy, debe crear un evento FPolicy. El evento se asocia a la política de FPolicy cuando se cree. Un evento define qué protocolo supervisar y qué eventos de acceso a archivos supervisar y filtrar.

Antes de empezar

Debe completar el evento de FPolicy "hoja de trabajo".

Cree el evento FPolicy

1. Cree el evento de FPolicy mediante `vserver fpolicy policy event create` el comando.

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -file-operations open,close,read,write
   ```

2. Verifique la configuración de eventos de FPolicy mediante `vserver fpolicy policy event show` el comando.

   ```
   vserver fpolicy policy event show -vserver vs1.example.com
   ```

   ```
                    Event                File                      Is Volume
   Vserver          Name      Protocols  Operations    Filters     Operation
   ---------------  --------- ---------  ------------- ---------
   ------------
   vs1.example.com  event1    cifs       open, close,  -           false
                                         read, write
   ```

Cree los eventos de acceso denegado a FPolicy

A partir de ONTAP 9.13.1, los usuarios pueden recibir notificaciones por operaciones de archivos fallidas debido a la falta de permisos. Estas notificaciones son valiosas para la seguridad, la protección contra el ransomware y la gobernanza.

1. Cree el evento de FPolicy mediante `vserver fpolicy policy event create` el comando.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name
event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

Crear almacenes persistentes de ONTAP FPolicy

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. A partir de ONTAP 9.14,1, FPolicy permite configurar "almacenes persistentes"para capturar eventos de acceso a archivos para políticas asíncronas no obligatorias en la SVM. No se admiten las configuraciones síncronas (obligatorias o no obligatorias) y asíncronas obligatorias.

A partir de ONTAP 9.15.1, se simplifica la configuración de almacén persistente de FPolicy. El `persistent-store create` comando automatiza la creación de volúmenes para la SVM y configura el volumen para el almacén persistente.

Hay dos formas de crear un almacén persistente, según la versión de ONTAP:

- ONTAP 9.15.1 o posterior: Cuando se crea el almacén persistente, ONTAP crea y configura automáticamente su volumen al mismo tiempo. Esto simplifica la configuración de almacén persistente de FPolicy e implementa todas las prácticas recomendadas.
- ONTAP 9.14.1: Cree y configure manualmente un volumen y, a continuación, cree un almacén persistente para el volumen recién creado.

Solo se puede configurar un almacén persistente en cada SVM. Es necesario usar este único almacén persistente para todas las configuraciones de FPolicy en dicho SVM, incluso si las políticas son de partners distintos.

Crear un almacén persistente (ONTAP 9.15.1 o posterior)

A partir de ONTAP 9.15,1, utilice `fpolicy persistent-store create` el comando para crear el almacén persistente de FPolicy con la creación y la configuración de volúmenes en línea. ONTAP bloquea automáticamente el volumen del acceso al protocolo de usuario externo (CIFS/NFS).

Antes de empezar

- La SVM donde desee crear el almacén persistente debe tener al menos un agregado.
- Debe tener acceso a los agregados disponibles de la SVM y suficientes permisos para crear volúmenes.

Pasos

1. Cree el almacén persistente, que crea y configura el volumen automáticamente:

```
vserver fpolicy persistent-store create -vserver <vserver> -persistent-store
<name> -volume <volume_name> -size <size> -autosize-mode
<off|grow|grow_shrink>
```

   - `vserver`El parámetro es el nombre de la SVM.
   - `persistent-store`El parámetro es el nombre del almacén persistente.

- `volume`El parámetro es el nombre del volumen de almacenamiento persistente.

  > Si desea utilizar un volumen existente vacío, use `volume show` el comando para encontrarlo y especificarlo en el parámetro volume.

- El `size` parámetro se basa en la duración del tiempo para el que desea continuar los eventos que no se entregan al servidor externo (aplicación asociada).

  Por ejemplo, si desea que 30 minutos de eventos persistan en un clúster con una capacidad de 30K notificaciones por segundo:

  Tamaño de volumen requerido = 30000 x 30 x 60 x 0,6KB (tamaño promedio de registro de notificación) = 32400000 KB = ~32 GB

  Para obtener la tasa de notificación aproximada, puede ponerse en contacto con su aplicación partner de FPolicy o usar el contador de FPolicy `requests_dispatched_rate` .

  > Si se utiliza un volumen existente, el parámetro size es opcional. Si se proporciona un valor para el parámetro size, se modificará el volumen con el tamaño que se especifique.

- `autosize-mode`El parámetro especifica el modo autosize del volumen. Los modos de ajuste de tamaño automático admitidos son:
  - Desactivado: El volumen no aumenta ni disminuye su tamaño en respuesta a la cantidad de espacio utilizado.
  - Crecer: El volumen crece automáticamente cuando el espacio utilizado en el volumen está por encima del umbral de crecimiento.
  - Grow_shrink: El volumen aumenta o reduce su tamaño en respuesta a la cantidad de espacio utilizado.

2. Cree la política de FPolicy y agregue el nombre del almacén persistente a esa política. Para obtener más información, consulte "Cree la política FPolicy".

Crear un almacén persistente (ONTAP 9.14.1)

Puede crear un volumen y, a continuación, crear un almacén persistente para utilizar ese volumen. Luego, se puede bloquear el volumen recién creado desde el acceso al protocolo de usuario externo (CIFS/NFS).

Pasos

1. Cree un volumen vacío en la SVM que se pueda aprovisionar para el almacén persistente:

   ```
   volume create -vserver <SVM Name> -volume <volume> -state <online> -policy
   <default> -unix-permissions <777> -size <value> -aggregate <aggregate name>
   -snapshot-policy <none>
   ```

   Se espera que un usuario administrador con suficiente Privileges de control de acceso basado en roles (para crear un volumen) cree un volumen (con los comandos de la cli del volumen o la API de REST) del tamaño deseado y proporcione el nombre de ese volumen como `-volume` en el almacén persistente create CLI o la API de REST.

   - `vserver`El parámetro es el nombre de la SVM.
   - `volume`El parámetro es el nombre del volumen de almacenamiento persistente.

- `state`El parámetro debe establecerse en línea para que el volumen esté disponible para su uso.
- `policy`El parámetro se establece en la política de servicio de FPolicy, si ya tiene una configurada. Si no es así, puede utilizar `volume modify` el comando más adelante para agregar la política.
- `unix-permissions`El parámetro es opcional.
- El `size` parámetro se basa en la duración del tiempo para el que desea continuar los eventos que no se entregan al servidor externo (aplicación asociada).

  Por ejemplo, si desea que 30 minutos de eventos persistan en un clúster con una capacidad de 30K notificaciones por segundo:

  Tamaño de volumen requerido = 30000 x 30 x 60 x 0,6KB (tamaño promedio de registro de notificación) = 32400000 KB = ~32 GB

Para obtener la tasa de notificación aproximada, puede ponerse en contacto con su aplicación partner de FPolicy o usar el contador de FPolicy `requests_dispatched_rate` .

- El parámetro de agregado es necesario para los volúmenes FlexVol; de lo contrario, no es necesario.
- `snapshot-policy`El parámetro debe definirse en none. Esto garantiza que no haya ninguna restauración accidental de la instantánea que provoque la pérdida de eventos actuales y evite el posible procesamiento de eventos duplicados.

  Si desea utilizar un volumen existente vacío, utilice `volume show` el comando para encontrarlo y `volume modify` el comando para realizar todas las alteraciones necesarias. Asegúrese de que la política, el tamaño y `snapshot-policy` los parámetros están definidos correctamente para el almacén persistente.

2. Cree el almacén persistente:

   ```
   vserver fpolicy persistent store create -vserver <SVM> -persistent-store
   <PS_name> -volume <volume>
   ```

   - `vserver`El parámetro es el nombre de la SVM.
   - `persistent-store`El parámetro es el nombre del almacén persistente.
   - `volume`El parámetro es el nombre del volumen de almacenamiento persistente.
3. Cree la política de FPolicy y agregue el nombre del almacén persistente a esa política. Para obtener más información, consulte "Cree la política FPolicy".

Crear políticas de ONTAP FPolicy

Cuando crea la política de FPolicy, debe asociar un motor externo y uno o varios eventos a la política. La directiva también especifica si es necesario realizar un tramado obligatorio, si los servidores FPolicy tienen un acceso privilegiado a los datos en la máquina virtual de almacenamiento (SVM) y si está habilitada la lectura paso a través para archivos sin conexión.

Antes de empezar

- Debe rellenar la hoja de trabajo de la política FPolicy.
- Si planea configurar la directiva para que utilice servidores FPolicy, el motor externo debe existir.

- Debe existir al menos un evento FPolicy que planifique para asociar a la política de FPolicy.
- Si desea configurar el acceso a datos con privilegios, debe existir un servidor SMB en la SVM.
- Para configurar un almacén persistente para una política, el tipo de motor debe ser **asincrónico** y la política debe ser **no obligatoria**.

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

Pasos

1. Cree la política de FPolicy:

   ```
   vserver fpolicy policy create -vserver-name vserver_name -policy-name
   policy_name -engine engine_name -events event_name, [-persistent-store
   PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
   privileged-user-name domain\user_name] [-is-passthrough-read-enabled
   {true|false}]
   ```

   - Puede añadir uno o varios eventos a la política de FPolicy.
   - De forma predeterminada, la selección obligatoria está activada.
   - Si desea permitir el acceso con privilegios definiendo el `-allow-privileged-access` parámetro en `yes`, también debe configurar un nombre de usuario con privilegios para el acceso con privilegios.
   - Si desea configurar passthrough-read definiendo el `-is-passthrough-read-enabled` parámetro en `true`, también debe configurar el acceso a datos con privilegios.

     El siguiente comando crea una política denominada «'poly1'» que tiene asociado el evento denominado «'event1'» y el motor externo denominado «'motor1'». Esta política utiliza valores predeterminados en la configuración de la política: `vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

     El siguiente comando crea una política denominada «'policy 2» que tiene asociado el evento denominado «'event2'» y el motor externo denominado «'motor2'». Esta directiva está configurada para utilizar acceso privilegiado utilizando el nombre de usuario especificado. La lectura PassThrough está habilitada:

     ```
     vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
     -events event2 -engine engine2 -allow-privileged-access yes -privileged-
     user-name example\archive_acct -is-passthrough-read-enabled true
     ```

     El siguiente comando crea una política denominada «'native1'» que tiene asociado el evento denominado «'event3'». Esta directiva utiliza el motor nativo y utiliza valores predeterminados en la configuración de directivas:

   ```
   vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
   -events event3 -engine native
   ```

2. Verifique la configuración de la política de FPolicy mediante `vserver fpolicy policy show` el comando.

   El siguiente comando muestra información acerca de las tres políticas de FPolicy configuradas, incluida la siguiente información:

   - La SVM asociada a la política

- El motor externo asociado a la directiva
- Los eventos asociados a la política
- Si es necesario realizar una selección obligatoria
- Indica si se necesita acceso con privilegios `vserver fpolicy policy show`

```
   Vserver       Policy     Events    Engine    Is Mandatory  Privileged
                 Name                                       Access
--------------   ---------  --------- --------- ------------
-----------
vs1.example.com  policy1    event1    engine1   true          no
vs1.example.com  policy2    event2    engine2   true          yes
vs1.example.com  native1    event3    native    true          no
```

Crear ámbitos de ONTAP FPolicy

Después de crear la política de FPolicy, debe crear un alcance de FPolicy. Al crear el ámbito, debe asociar el ámbito a una política de FPolicy. Un ámbito define los límites en los que se aplica la política de FPolicy. Los ámbitos pueden incluir o excluir archivos basados en recursos compartidos, políticas de exportación, volúmenes y extensiones de archivo.

Antes de empezar

Se debe completar la hoja de cálculo del alcance de FPolicy. La política de FPolicy debe existir con un motor externo asociado (si la política se configura para utilizar servidores de FPolicy externos) y debe tener al menos un evento de FPolicy asociado.

Pasos

1. Cree el ámbito de FPolicy mediante `vserver fpolicy policy scope create` el comando.

   ```
   vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name
   policy1 -volumes-to-include datavol1,datavol2
   ```

2. Verifique la configuración de alcance de FPolicy mediante `vserver fpolicy policy scope show` el comando.

   ```
   vserver fpolicy policy scope show -vserver vs1.example.com -instance
   ```

```
                    Vserver: vs1.example.com
                     Policy: policy1
          Shares to Include: -
          Shares to Exclude: -
         Volumes to Include: datavol1, datavol2
         Volumes to Exclude: -
Export Policies to Include: -
Export Policies to Exclude: -
File Extensions to Include: -
File Extensions to Exclude: -
```

Habilitar políticas de ONTAP FPolicy

Después de configurar una configuración de políticas de FPolicy, debe habilitar la política de FPolicy. Al habilitar la directiva, se establece su prioridad e inicia la supervisión del acceso a los archivos de la directiva.

Antes de empezar

La política de FPolicy debe existir con un motor externo asociado (si la política se configura para utilizar servidores de FPolicy externos) y debe tener al menos un evento de FPolicy asociado. El alcance de la política de FPolicy debe existir y debe asignarse a la política de FPolicy.

Acerca de esta tarea

La prioridad se utiliza cuando se habilitan varias políticas en la máquina virtual de almacenamiento (SVM) y se ha suscrito más de una directiva al mismo evento de acceso a archivos. Las directivas que utilizan la configuración del motor nativo tienen una prioridad mayor que las directivas para cualquier otro motor, independientemente del número de secuencia que se les haya asignado al habilitar la política.

No se puede habilitar una política en la SVM de administrador.

Pasos

1. Habilite la política de FPolicy mediante `vserver fpolicy enable` el comando.

   ```
   vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
   -sequence-number 1
   ```

2. Compruebe que la política de FPolicy esté habilitada mediante `vserver fpolicy show` el comando.

   ```
   vserver fpolicy show -vserver vs1.example.com
   ```

   ```
                                    Sequence
   Vserver          Policy Name       Number  Status   Engine
   ---------------  ----------------- --------  -------- ---------
   vs1.example.com  policy1                1  on       engine1
   ```

Gestione las configuraciones de FPolicy

Modifique las configuraciones de FPolicy

Comandos que modifican configuraciones de FPolicy en ONTAP

Puede modificar las configuraciones de FPolicy modificando los elementos que componen la configuración. Puede modificar motores externos, eventos de FPolicy, ámbitos de FPolicy, almacenes persistentes de FPolicy y políticas de FPolicy. También es posible habilitar o deshabilitar las políticas de FPolicy. Al deshabilitar la política de FPolicy, la supervisión de archivos se interrumpirá para esa política.

Debe deshabilitar una política de FPolicy antes de modificar su configuración.

Si desea modificar…	Se usa este comando…
Motores externos	`vserver fpolicy policy external-engine modify`
Eventos	`vserver fpolicy policy event modify`
Ámbitos	`vserver fpolicy policy scope modify`
Almacenamiento persistente	`vserver fpolicy persistent-store modify`
Normativas	`vserver fpolicy policy modify`

Obtenga más información sobre `vserver fpolicy policy` en el "Referencia de comandos del ONTAP".

Habilitar o deshabilitar las políticas de ONTAP FPolicy

Es posible habilitar las políticas de FPolicy una vez completada la configuración. Al habilitar la directiva, se establece su prioridad e inicia la supervisión del acceso a los archivos de la directiva. Puede deshabilitar las políticas de FPolicy si desea detener la supervisión de acceso a los archivos para la política.

Antes de empezar

Antes de habilitar las políticas de FPolicy, debe completar la configuración de FPolicy.

Acerca de esta tarea

- La prioridad se utiliza cuando se habilitan varias políticas en la máquina virtual de almacenamiento (SVM) y se ha suscrito más de una directiva al mismo evento de acceso a archivos.
- Las directivas que utilizan la configuración del motor nativo tienen una prioridad mayor que las directivas para cualquier otro motor, independientemente del número de secuencia que se les haya asignado al habilitar la política.
- Si desea cambiar la prioridad de una política de FPolicy, debe deshabilitar la política y volver a habilitarla mediante el nuevo número de secuencia.

Paso

1. Ejecute la acción adecuada:

Si desea…	Introduzca el siguiente comando…
Habilite una política de FPolicy	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`
Deshabilite una política de FPolicy	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

Mostrar información acerca de las configuraciones de FPolicy

Obtenga información sobre los comandos show de ONTAP FPolicy

Resulta útil cuando se muestra información sobre la configuración de FPolicy para comprender cómo `show` funcionan los comandos.

Un `show` comando sin parámetros adicionales muestra información en un formulario de resumen. Además, cada `show` comando tiene los mismos dos parámetros opcionales mutuamente excluyentes, `-instance` y `-fields`.

Cuando se utiliza `-instance` el parámetro con un `show` comando, el resultado del comando muestra información detallada en formato de lista. En algunos casos, el resultado detallado puede ser largo e incluir más información de la que usted necesita. Puede usar el `-fields fieldname[,fieldname…]` parámetro para personalizar la salida de modo que muestre información solo de los campos especificados. Puede identificar los campos que puede especificar introduciendo `?` después del `-fields` parámetro.

El resultado de un `show` comando con el `-fields` parámetro puede mostrar otros campos relevantes y necesarios relacionados con los campos solicitados.

`show`Cada comando tiene uno o varios parámetros opcionales que filtran ese resultado y le permiten limitar el alcance de la información mostrada en la salida de comandos. Puede identificar qué parámetros opcionales están disponibles para un comando introduciendo `?` después del `show` comando.

`show`El comando soporta patrones de estilo UNIX y comodines para permitir que coincida con varios valores en argumentos de parámetros de comando. Por ejemplo, puede utilizar el operador comodín (*), EL operador NOT (!), EL operador OR (|), el operador Range (integer...integer), el operador menor que (<), el operador mayor que (>), el operador menor o igual que (\<=) y el operador mayor que o igual a (>=) cuando especifique valores.

Para obtener más información sobre el uso de patrones de estilo UNIX y comodines, consulte la Mediante la

interfaz de línea de comandos de la ONTAP.

Comandos para mostrar información sobre las configuraciones de FPolicy en ONTAP

Puede utilizar `fpolicy show` los comandos para mostrar información sobre la configuración de FPolicy, incluida información sobre motores externos, eventos, ámbitos y políticas de FPolicy.

Si desea mostrar información acerca de FPolicy…	Se usa este comando…
Motores externos	`vserver fpolicy policy external-engine show`
Eventos	`vserver fpolicy policy event show`
Ámbitos	`vserver fpolicy policy scope show`
Normativas	`vserver fpolicy policy show`

Obtenga más información sobre `vserver fpolicy policy` en el "Referencia de comandos del ONTAP".

Mostrar información sobre el estado de la política de ONTAP FPolicy

Puede mostrar información acerca del estado de las políticas de FPolicy para determinar si una política está habilitada, qué motor externo está configurado para usar, qué número de secuencia corresponde a la política y a qué máquina virtual de almacenamiento (SVM) está asociada la política de FPolicy.

Acerca de esta tarea

Si no especifica ningún parámetro, el comando muestra la siguiente información:

- Nombre de SVM
- Nombre de la política
- Número de secuencia de directivas
- Estado de la política

Además de mostrar información sobre el estado de política para las políticas de FPolicy configuradas en el clúster o una SVM específica, puede usar parámetros de comandos para filtrar el resultado del comando por otros criterios.

Puede especificar `-instance` el parámetro para mostrar información detallada sobre las políticas enumeradas. Como alternativa, puede usar el `-fields` parámetro para mostrar solo los campos indicados en el resultado del comando o `-fields ?` para determinar qué campos puede usar.

Paso

1. Mostrar información filtrada acerca del estado de política de FPolicy mediante el comando correspondiente:

Si desea mostrar información de estado acerca de políticas…	Introduzca el comando…
En el clúster	`vserver fpolicy show`
Que tienen el estado especificado	`vserver fpolicy show -status {on
off}`	En una SVM especificada
`vserver fpolicy show -vserver vserver_name`	Con el nombre de la política especificada
`vserver fpolicy show -policy-name policy_name`	Que utilizan el motor externo especificado

Ejemplo

En el siguiente ejemplo se muestra la información acerca de las políticas de FPolicy en el clúster:

```
cluster1::> vserver fpolicy show
                                      Sequence
Vserver              Policy Name        Number  Status      Engine
-------------------- ------------------ --------  ---------   ---------
FPolicy              cserver_policy     -         off         eng1
vs1.example.com      v1p1               -         off         eng2
vs1.example.com      v1p2               -         off         native
vs1.example.com      v1p3               -         off         native
vs1.example.com      cserver_policy     -         off         eng1
vs2.example.com      v1p1               3         on          native
vs2.example.com      v1p2               1         on          eng3
vs2.example.com      cserver_policy     2         on          eng1
```

Mostrar información sobre las políticas FPolicy de ONTAP habilitadas

Puede mostrar información acerca de las políticas de FPolicy habilitadas para determinar qué motor externo de FPolicy se ha configurado para utilizar, cuál es la prioridad de la política y a qué máquina virtual de almacenamiento (SVM) está asociada la política de FPolicy.

Acerca de esta tarea

Si no especifica ningún parámetro, el comando muestra la siguiente información:

- Nombre de SVM
- Nombre de la política
- Prioridad en materia de políticas

Puede utilizar parámetros de comando para filtrar el resultado del comando por criterios especificados.

Paso

1. Muestre información sobre las políticas de FPolicy habilitadas mediante el comando correspondiente:

Si desea mostrar información sobre las políticas habilitadas…	Introduzca el comando…
En el clúster	`vserver fpolicy show-enabled`
En una SVM especificada	`vserver fpolicy show-enabled -vserver vserver_name`
Con el nombre de la política especificada	`vserver fpolicy show-enabled -policy-name policy_name`
Con el número de secuencia especificado	`vserver fpolicy show-enabled -priority integer`

Ejemplo

En el siguiente ejemplo se muestra la información acerca de las políticas de FPolicy habilitadas en el clúster:

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

Gestione las conexiones del servidor FPolicy

Conéctese a servidores externos de FPolicy en ONTAP

Para habilitar el procesamiento de archivos, es posible que deba conectarse manualmente a un servidor FPolicy externo si la conexión ha finalizado previamente. Una conexión se completa después de alcanzar el tiempo de espera del servidor o debido a algún error. Como alternativa, el administrador podría terminar manualmente una conexión.

Acerca de esta tarea

Si se produce un error grave, es posible finalizar la conexión con el servidor FPolicy. Después de resolver el problema que provocó el error grave, debe volver a conectarse manualmente al servidor FPolicy.

Pasos

1. Conéctese al servidor FPolicy externo mediante `vserver fpolicy engine-connect` el comando.

Obtenga más información sobre `vserver fpolicy engine-connect` en el "Referencia de comandos del ONTAP".

2. Compruebe que el servidor FPolicy externo está conectado mediante `vserver fpolicy show-engine` el comando.

   Obtenga más información sobre `vserver fpolicy show-engine` en el "Referencia de comandos del ONTAP".

Desconéctese de los servidores externos de FPolicy en ONTAP

Es posible que deba desconectarse manualmente de un servidor de FPolicy externo. Esto puede ser aconsejable si el servidor FPolicy tiene problemas con el procesamiento de solicitudes de notificación o si necesita realizar tareas de mantenimiento en el servidor FPolicy.

Pasos

1. Desconéctese del servidor FPolicy externo con `vserver fpolicy engine-disconnect` el comando.

   Obtenga más información sobre `vserver fpolicy engine-disconnect` en el "Referencia de comandos del ONTAP".

2. Compruebe que el servidor FPolicy externo está desconectado mediante `vserver fpolicy show-engine` el comando.

   Obtenga más información sobre `vserver fpolicy show-engine` en el "Referencia de comandos del ONTAP".

Mostrar información sobre las conexiones a servidores FPolicy externos de ONTAP

Es posible mostrar información de estado acerca de las conexiones a servidores FPolicy externos (servidores FPolicy) para el clúster o para una máquina virtual de almacenamiento (SVM) especificada. Esta información puede ayudarle a determinar qué servidores de FPolicy están conectados.

Acerca de esta tarea

Si no especifica ningún parámetro, el comando muestra la siguiente información:

- Nombre de SVM
- Nombre del nodo
- Nombre de la política de FPolicy
- Dirección IP del servidor FPolicy
- Estado del servidor FPolicy
- Tipo de servidor FPolicy

Además de mostrar información acerca de las conexiones de FPolicy en el clúster o una SVM específica, puede usar parámetros de comandos para filtrar el resultado del comando según otros criterios.

Puede especificar `-instance` el parámetro para mostrar información detallada sobre las políticas enumeradas. Como alternativa, puede usar el `-fields` parámetro para mostrar solo los campos indicados en el resultado del comando. Puede introducir `?` después del `-fields` parámetro para averiguar qué campos puede usar.

Paso

1. Mostrar información filtrada acerca del estado de conexión entre el nodo y el servidor FPolicy mediante el comando correspondiente:

Si desea mostrar información de estado de conexión acerca de los servidores FPolicy…	Introduzca…
Que especifique	`vserver fpolicy show-engine -server IP_address`
Para una SVM especificada	`vserver fpolicy show-engine -vserver vserver_name`
Que se adjuntan con una directiva específica	`vserver fpolicy show-engine -policy-name policy_name`
Con el estado del servidor que especifique	`vserver fpolicy show-engine -server-status status` El estado del servidor puede ser uno de los siguientes: • `connected` • `disconnected` • `connecting` • `disconnecting`
Con el tipo especificado	`vserver fpolicy show-engine -server-type type` El tipo de servidor FPolicy puede ser uno de los siguientes: • `primary` • `secondary`

Que se desconectaron con el motivo especificado	`vserver fpolicy show-engine -disconnect-reason text` La desconexión puede deberse a varias razones. Los siguientes son motivos comunes para la desconexión: • `Disconnect command received from CLI.` • `Error encountered while parsing notification response from FPolicy server.` • `FPolicy Handshake failed.` • `SSL handshake failed.` • `TCP Connection to FPolicy server failed.` • `The screen response message received from the FPolicy server is not valid.`

Ejemplo

Este ejemplo muestra información acerca de las conexiones del motor externo a los servidores FPolicy en SVM vs1.example.com:

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                              Server-       Server-
Vserver         Policy    Node         Server        status        type
--------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1   node1        10.1.1.2      connected     primary
vs1.example.com policy1   node1        10.1.1.3      disconnected  primary
vs1.example.com policy1   node2        10.1.1.2      connected     primary
vs1.example.com policy1   node2        10.1.1.3      disconnected  primary
```

Este ejemplo solo muestra información acerca de los servidores FPolicy conectados:

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver         policy-name server
---------- --------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2
```

Mostrar información sobre el estado de la conexión de lectura directa de ONTAP FPolicy

Es posible mostrar información acerca del estado de conexión de lectura directa de FPolicy en los servidores FPolicy externos (servidores FPolicy) para el clúster o para una

máquina virtual de almacenamiento (SVM) especificada. Esta información puede ayudarle a determinar qué servidores de FPolicy tienen conexiones de datos de lectura directa y para los que se ha desconectado los servidores de FPolicy.

Acerca de esta tarea

Si no especifica ningún parámetro, el comando muestra la siguiente información:

- Nombre de SVM
- Nombre de la política de FPolicy
- Nombre del nodo
- Dirección IP del servidor FPolicy
- Estado de conexión de lectura directa de FPolicy

Además de mostrar información acerca de las conexiones de FPolicy en el clúster o una SVM específica, puede usar parámetros de comandos para filtrar el resultado del comando según otros criterios.

Puede especificar `-instance` el parámetro para mostrar información detallada sobre las políticas enumeradas. Como alternativa, puede usar el `-fields` parámetro para mostrar solo los campos indicados en el resultado del comando. Puede introducir `?` después del `-fields` parámetro para averiguar qué campos puede usar.

Paso

1. Mostrar información filtrada acerca del estado de conexión entre el nodo y el servidor FPolicy mediante el comando correspondiente:

Si desea mostrar información sobre el estado de la conexión acerca de…	Introduzca el comando…
El estado de la conexión de lectura directa de FPolicy para el clúster	`vserver fpolicy show-passthrough-read-connection`
El estado de conexión de lectura directa de FPolicy para una SVM especificada	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`
Estado de conexión de lectura directa de FPolicy para una política especificada	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
El estado de conexión de lectura directa de FPolicy detallado para una política especificada	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`

El estado de conexión de lectura directa de FPolicy correspondiente al estado especificado	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status` El estado del servidor puede ser uno de los siguientes: • `connected` • `disconnected`

Ejemplo

El siguiente comando muestra información acerca de las conexiones de lectura de paso a través de todos los servidores FPolicy del clúster:

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                          FPolicy           Server
Vserver          Policy Name   Node         Server            Status
---------------  ------------- ------------ -----------------
--------------
vs2.example.com  pol_cifs_2    FPolicy-01   2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
```

El siguiente comando muestra información detallada acerca de las conexiones de lectura a través de paso desde los servidores FPolicy configurados en la política "'pol_cifs_1'":

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                       Node: FPolicy-01
                                    Vserver: vs1.example.com
                                     Policy: pol_cifs_1
                                     Server: 1.1.1.1
               Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```