Cree la configuración de FPolicy

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Cree la configuración de FPolicy

Cree el motor externo 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.

Lo que necesitará

La "motor externo" debe rellenar la hoja de trabajo.

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 FPolicy mediante `vserver fpolicy policy external-engine create` 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. Verifique la configuración del motor externo de FPolicy mediante `vserver fpolicy policy external-engine show` 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: -
```

Cree el evento 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 FPolicy mediante `vserver fpolicy policy event create` 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 del evento FPolicy mediante `vserver fpolicy policy event show` 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 FPolicy mediante `vserver fpolicy policy event create` 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

A partir de ONTAP 9.14.1, FPolicy le permite configurar un "Almacenes persistentes" 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.

Mejores prácticas

- Antes de utilizar la funcionalidad de almacén persistente, asegúrese de que sus aplicaciones asociadas admiten esta configuración.
- El volumen de almacenamiento persistente se configura por SVM. Para cada SVM con FPolicy necesitará un volumen de almacenamiento persistente.
- El nombre del volumen de almacenamiento persistente y la ruta de unión especificada en el momento de la creación del volumen deben coincidir.
- Cree el volumen de almacenamiento persistente en el nodo con LIF que esperan que Fpolicy supervise el tráfico máximo.
- Establezca la política de Snapshot en `none` para ese volumen en lugar de `default`. De este modo se garantiza que no haya ninguna restauración accidental de la instantánea que provoque la pérdida de eventos actuales y que se evite un posible procesamiento de eventos duplicados.
- Haga que el volumen de almacenamiento persistente no sea accesible para el acceso del protocolo de usuario externo (CIFS/NFS) y evite daños o eliminación accidentales de los registros de eventos persistentes. Para lograr esto, después de habilitar FPolicy, desmonte el volumen en ONTAP para eliminar la ruta de unión, esto hace que sea inaccesible para el acceso al protocolo de usuario.

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> -junction
   -path <path> -policy <default> -unix-permissions <777> -size <value>
   -aggregate <aggregate name> -snapshot-policy <none>
   ```

   - El tamaño del volumen de almacenamiento persistente se basa en la duración del tiempo durante el cual 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 medio de registro de notificación) = 32400000 KB = ~32 GB

Para encontrar la tasa de notificación aproximada, puede contactar con su aplicación de partner de FPolicy o utilizar el contador de FPolicy `requests_dispatched_rate`.

- Se espera que un usuario administrador con suficientes privilegios de RBAC (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 el `-volume` En el almacén persistente create el comando de la CLI o la API de REST.

2. Cree el almacén persistente:

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

   - Persistent-store: Nombre del almacén persistente
   - Volume: El volumen de almacenamiento persistente

3. Una vez creado el almacén persistente, puede crear la política de FPolicy y agregar el nombre del almacén persistente a esa política. Para obtener más información, consulte "Cree la política FPolicy".

Cree la política 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.

Lo que necesitará

- 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 mediante la configuración del `-allow-privileged -access` parámetro a. `yes`, también debe configurar un nombre de usuario con privilegios para el acceso con privilegios.
- Si desea configurar passthrough-read mediante el ajuste `-is-passthrough-read-enabled` parámetro a. `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 directiva utiliza valores predeterminados en la configuración de directivas: `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. Compruebe la configuración de la política de FPolicy mediante la `vserver fpolicy policy show` 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
   - Si se requiere un acceso privilegiado `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
```

Cree el alcance de 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.

Lo que necesitará

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 alcance de FPolicy mediante `vserver fpolicy policy scope create` comando.

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

2. Compruebe la configuración del alcance de FPolicy mediante `vserver fpolicy policy scope show` 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: -
   ```

Habilite la política de 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.

Lo que necesitará

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` 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 el `vserver fpolicy show` comando.

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

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