Planifique la configuración externa del motor de FPolicy

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Planifique la configuración externa del motor de FPolicy . . . 1
Configuraciones del motor externo de Plan ONTAP FPolicy . . . 1
Información que se define al crear el motor externo de FPolicy . . . 1
Cuáles son los parámetros básicos del motor externo . . . 2
Cuáles son las opciones avanzadas del motor externo . . . 5
Información adicional sobre la configuración de los motores externos de ONTAP FPolicy para utilizar conexiones autenticadas SSL . . . 8
Autenticación de servidor SSL . . . 8
Autenticación mutua . . . 8
Instalar certificados para SSL . . . 8
Los certificados FPolicy de ONTAP no se replican en relaciones de recuperación ante desastres de SVM con una configuración que no preserva la ID . . . 8
Restricciones para motores externos de ONTAP FPolicy con ámbito de clúster con configuraciones de recuperación ante desastres de MetroCluster y SVM . . . 9
Hojas de trabajo completas de configuración del motor externo de ONTAP FPolicy . . . 9
Información para una configuración básica externa del motor . . . 10
Información para parámetros avanzados del motor externo . . . 10

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		