Planeie a configuração FPolicy

ONTAP 9

NetApp
January 17, 2025

Índice

Planeie a configuração FPolicy

Requisitos, considerações e práticas recomendadas para configurar o FPolicy

Antes de criar e configurar configurações FPolicy em suas máquinas virtuais de armazenamento (SVMs), você precisa estar ciente de certos requisitos, considerações e práticas recomendadas para configurar o FPolicy.

Os recursos de FPolicy são configurados por meio da interface de linha de comando (CLI) ou por meio de APIs REST.

Requisitos para configurar FPolicy

Antes de configurar e ativar o FPolicy na máquina virtual de storage (SVM), você precisa estar ciente de certos requisitos.

- Todos os nós no cluster devem estar executando uma versão do ONTAP que suporte FPolicy.
- Se você não estiver usando o mecanismo FPolicy nativo do ONTAP, você deve ter servidores FPolicy externos instalados.
- Os servidores FPolicy devem ser instalados em um servidor acessível a partir das LIFs de dados do SVM onde as políticas FPolicy estão ativadas.

> A partir do ONTAP 9.8, o ONTAP fornece um serviço de LIF cliente para conexões FPolicy de saída com a adição `data-fpolicy-client` do serviço. "Saiba mais sobre LIFs e políticas de serviço".

- O endereço IP do servidor FPolicy deve ser configurado como um servidor primário ou secundário na configuração do mecanismo externo da política FPolicy.
- Se os servidores FPolicy acessarem dados em um canal de dados privilegiado, os seguintes requisitos adicionais devem ser atendidos:
  - O SMB deve ser licenciado no cluster.

    O acesso privilegiado a dados é realizado usando conexões SMB.
  - Uma credencial de usuário deve ser configurada para acessar arquivos pelo canal de dados privilegiado.
  - O servidor FPolicy deve ser executado sob as credenciais configuradas na configuração FPolicy.
  - Todos os LIFs de dados usados para se comunicar com os servidores FPolicy devem ser configurados para ter `cifs` como um dos protocolos permitidos.

    Isso inclui os LIFs usados para conexões de passagem-leitura.

Práticas recomendadas e recomendações ao configurar o FPolicy

Ao configurar o FPolicy em máquinas virtuais de armazenamento (SVMs), familiarize-se com as práticas recomendadas e recomendações gerais de configuração para garantir que sua configuração do FPolicy forneça desempenho de monitoramento robusto e resultados que atendam aos seus requisitos.

Para diretrizes específicas relacionadas a desempenho, dimensionamento e configuração, trabalhe com seu aplicativo de parceiro FPolicy.

Armazenamentos persistentes

A partir do ONTAP 9.14,1, o FPolicy permite configurar um armazenamento persistente para capturar eventos de acesso a arquivos para políticas assíncronas não obrigatórias no SVM. Armazenamentos persistentes podem ajudar a desacoplar o processamento de e/S do cliente do processamento de notificações FPolicy para reduzir a latência do cliente. Configurações síncronas (obrigatórias ou não obrigatórias) e assíncronas obrigatórias não são suportadas.

- Antes de usar a funcionalidade de armazenamento persistente, certifique-se de que as aplicações de parceiros suportem esta configuração.
- Você precisa de um armazenamento persistente para cada SVM em que o FPolicy esteja ativado.
  - Apenas um armazenamento persistente pode ser configurado em cada SVM. Esse único armazenamento persistente precisa ser usado em todas as configurações de FPolicy nesse SVM, mesmo que as políticas sejam de parceiros diferentes.
- ONTAP 9.15,1 ou posterior:
  - O armazenamento persistente, seu volume e sua configuração de volume são tratados automaticamente quando você cria o armazenamento persistente.
- ONTAP 9.14,1:
  - O armazenamento persistente, seu volume e sua configuração de volume são manipulados manualmente.
- Crie o volume de armazenamento persistente no nó com LIFs que esperam que o tráfego máximo seja monitorado pelo FPolicy.
  - ONTAP 9.15,1 ou posterior: Os volumes são criados e configurados automaticamente durante a criação do armazenamento persistente.
  - ONTAP 9.14,1: Os administradores de cluster precisam criar e configurar um volume para o armazenamento persistente em cada SVM em que o FPolicy está ativado.
- Se as notificações acumuladas no armazenamento persistente excederem o tamanho do volume provisionado, o FPolicy começa a deixar cair a notificação recebida com mensagens EMS apropriadas.
  - ONTAP 9.15,1 ou posterior: Além do `size` parâmetro, o `autosize-mode` parâmetro pode ajudar o volume a crescer ou diminuir em resposta à quantidade de espaço usado.
  - ONTAP 9.14,1: O `size` parâmetro é configurado durante a criação do volume para fornecer um limite máximo.
- Defina a política de instantâneos como `none` para o volume de armazenamento persistente em vez `default` de . Isso serve para garantir que não haja restauração acidental do snapshot levando à perda de eventos atuais e para evitar possível processamento de eventos duplicados.
  - ONTAP 9.15,1 ou posterior: O `snapshot-policy` parâmetro é configurado automaticamente como nenhum durante a criação de armazenamento persistente.
  - ONTAP 9.14,1: O `snapshot-policy` parâmetro é configurado `none` durante a criação do volume.
- Torne o volume de armazenamento persistente inacessível para acesso de protocolo de usuário externo (CIFS/NFS) para evitar corrupção acidental ou exclusão dos Registros de eventos persistentes.
  - ONTAP 9.15,1 ou posterior: O ONTAP bloqueia automaticamente o volume do acesso de protocolo de usuário externo (CIFS/NFS) durante a criação do armazenamento persistente.

- ONTAP 9.14,1: Depois de ativar o FPolicy, desmonte o volume no ONTAP para remover o caminho de junção. Isso o torna inacessível para acesso de protocolo de usuário externo (CIFS/NFS).

Para obter mais informações, "Armazenamentos persistentes de FPolicy"consulte e "Crie armazenamentos persistentes".

Failover de armazenamento persistente e giveback

O armazenamento persistente permanece como era quando o último evento foi recebido, quando há uma reinicialização inesperada ou FPolicy é desativado e ativado novamente. Após uma operação de takeover, novos eventos são armazenados e processados pelo nó do parceiro. Após uma operação de giveback, o armazenamento persistente retoma o processamento de quaisquer eventos não processados que possam permanecer de quando a aquisição do nó ocorreu. Os eventos ao vivo teriam prioridade sobre eventos não processados.

Se o volume de armazenamento persistente passar de um nó para outro no mesmo SVM, as notificações que ainda não foram processadas também serão movidas para o novo nó. Você precisa executar novamente `fpolicy persistent-store create` o comando em qualquer nó após o volume ser movido para garantir que as notificações pendentes sejam entregues ao servidor externo.

Configuração da política

A configuração do mecanismo externo FPolicy, eventos e escopo para SVMs pode melhorar sua experiência e segurança geral.

- Configuração do mecanismo externo FPolicy para SVMs:
  - Fornecer segurança adicional vem com um custo de desempenho. Ativar a comunicação SSL (Secure Sockets Layer) tem um efeito de desempenho no acesso a compartilhamentos.
  - O mecanismo externo FPolicy deve ser configurado com mais de um servidor FPolicy para fornecer resiliência e alta disponibilidade de processamento de notificações do servidor FPolicy.
- Configuração de eventos FPolicy para SVMs:

  O monitoramento das operações de arquivos influencia sua experiência geral. Por exemplo, filtrar as operações de arquivos indesejados no lado do armazenamento melhora sua experiência. A NetApp recomenda configurar a seguinte configuração:

  - Monitorar os tipos mínimos de operações de arquivos e permitir o número máximo de filtros sem quebrar o caso de uso.
  - Usando filtros para operações getattr, ler, escrever, abrir e fechar. Os ambientes de diretório base SMB e NFS têm uma alta porcentagem dessas operações.
- Configuração do escopo de FPolicy para SVMs:

  Restrinja o escopo das políticas aos objetos de storage relevantes, como compartilhamentos, volumes e exportações, em vez de habilitá-los em todo o SVM. O NetApp recomenda verificar as extensões do diretório. Se o `is-file-extension-check-on-directories-enabled` parâmetro estiver definido como `true`, os objetos de diretório serão submetidos às mesmas verificações de extensão que os arquivos normais.

Configuração de rede

A conetividade de rede entre o servidor FPolicy e o controlador deve ser de baixa latência. A NetApp recomenda separar o tráfego FPolicy do tráfego do cliente usando uma rede privada.

Além disso, você deve colocar servidores FPolicy externos (servidores FPolicy) próximo ao cluster com conetividade de alta largura de banda para fornecer latência mínima e conetividade de alta largura de banda.

> Para um cenário em que o LIF para tráfego FPolicy é configurado em uma porta diferente para o LIF para tráfego de cliente, o FPolicy LIF pode falhar para o outro nó devido a uma falha de porta. Como resultado, o servidor FPolicy torna-se inacessível a partir do nó, o que faz com que as notificações FPolicy para operações de arquivo no nó falhem. Para evitar esse problema, verifique se o servidor FPolicy pode ser acessado por pelo menos um LIF no nó para processar solicitações FPolicy para as operações de arquivo executadas nesse nó.

Configuração de hardware

Você pode ter o servidor FPolicy em um servidor físico ou virtual. Se o servidor FPolicy estiver em um ambiente virtual, você deverá alocar recursos dedicados (CPU, rede e memória) ao servidor virtual.

A taxa de servidor nó para FPolicy do cluster deve ser otimizada para garantir que os servidores FPolicy não estejam sobrecarregados, o que pode introduzir latências quando o SVM responder às solicitações do cliente. A proporção ideal depende do aplicativo parceiro para o qual o servidor FPolicy está sendo usado. A NetApp recomenda trabalhar com parceiros para determinar o valor apropriado.

Configuração de várias políticas

A política de FPolicy para bloqueio nativo tem a prioridade mais alta, independentemente do número de sequência, e as políticas de alteração de decisões têm uma prioridade mais alta do que outras. A prioridade da política depende do caso de uso. A NetApp recomenda trabalhar com parceiros para determinar a prioridade apropriada.

Considerações de tamanho

O FPolicy executa monitoramento em linha de operações SMB e NFS, envia notificações para o servidor externo e aguarda uma resposta, dependendo do modo de comunicação do motor externo (síncrono ou assíncrono). Esse processo afeta o desempenho dos recursos de CPU e acesso SMB e NFS.

Para mitigar quaisquer problemas, a NetApp recomenda trabalhar com parceiros para avaliar e dimensionar o ambiente antes de habilitar o FPolicy. O desempenho é afetado por vários fatores, incluindo o número de usuários, caraterísticas da carga de trabalho, como operações por usuário e tamanho de dados, latência de rede e falha ou lentidão do servidor.

Monitorar o desempenho

FPolicy é um sistema baseado em notificações. As notificações são enviadas para um servidor externo para processamento e para gerar uma resposta de volta ao ONTAP. Esse processo de ida e volta aumenta a latência para o acesso do cliente.

O monitoramento dos contadores de desempenho no servidor FPolicy e no ONTAP oferece a capacidade de identificar gargalos na solução e ajustar os parâmetros conforme necessário para uma solução ideal. Por exemplo, um aumento na latência de FPolicy tem um efeito em cascata na latência de acesso SMB e NFS. Portanto, você deve monitorar a carga de trabalho (SMB e NFS) e a latência do FPolicy. Além disso, você pode usar políticas de qualidade do serviço no ONTAP para configurar um workload para cada volume ou SVM habilitado para FPolicy.

O NetApp recomenda executar o `statistics show –object workload` comando para exibir estatísticas de carga de trabalho. Além disso, você deve monitorar os seguintes parâmetros:

- Latências médias, de leitura e de gravação
- Número total de operações
- Contadores de leitura e escrita

Você pode monitorar o desempenho dos subsistemas FPolicy usando os seguintes contadores FPolicy.

Você deve estar no modo de diagnóstico para coletar estatísticas relacionadas ao FPolicy.

Passos

1. Recolher contadores 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. Visualizar contadores FPolicy:
   a. `statistics show -object fpolicy –instance instance_name -sample-id ID`
   b. `statistics show -object fpolicy_server –instance instance_name -sample-id ID`

   Os `fpolicy` contadores e `fpolicy_server` fornecem informações sobre vários parâmetros de desempenho descritos na tabela a seguir.

Contadores	Descrição
• contadores de "fpolicy"*	aborted_requests
Número de solicitações de tela para as quais o processamento é abortado no SVM	event_count
Lista de eventos que resultam em notificação	max_request_latency
Latência máxima de solicitações de tela	pedidos_pendentes
Número total de solicitações de tela em andamento	processed_requests
Número total de solicitações de tela que passaram pelo processamento de fpolicy no SVM	request_latency_hist
Histograma de latência para solicitações de tela	requests_despached_rate
Número de solicitações de tela enviadas por segundo	requests_received_rate

Contadores	Descrição
Número de solicitações de tela recebidas por segundo	• contadores de "fpolicy_server"*
max_request_latency	Latência máxima para uma solicitação de tela
pedidos_pendentes	Número total de solicitações de tela aguardando resposta
request_latency (latência_de	Latência média para solicitação de tela
request_latency_hist	Histograma de latência para solicitações de tela
request_sent_rate	Número de solicitações de tela enviadas ao servidor FPolicy por segundo
taxa de resposta_recebida	Número de respostas de tela recebidas do servidor FPolicy por segundo

Gerencie o fluxo de trabalho FPolicy e a dependência de outras tecnologias

A NetApp recomenda desativar uma política de FPolicy antes de fazer quaisquer alterações de configuração. Por exemplo, se você quiser adicionar ou modificar um endereço IP no mecanismo externo configurado para a política ativada, desative primeiro a política.

Se você configurar o FPolicy para monitorar volumes do NetApp FlexCache, o NetApp recomenda que você não configure o FPolicy para monitorar as operações de arquivos de leitura e getattr. O monitoramento dessas operações no ONTAP requer a recuperação de dados inode-to-path (I2P). Como os dados I2P não podem ser recuperados de volumes FlexCache, eles devem ser recuperados do volume de origem. Portanto, o monitoramento dessas operações elimina os benefícios de desempenho que o FlexCache pode oferecer.

Quando o FPolicy e uma solução antivírus off-box são implantados, a solução antivírus recebe notificações primeiro. O processamento de FPolicy é iniciado somente após a verificação antivírus estar concluída. É importante que você dimensione as soluções antivírus corretamente porque um scanner antivírus lento pode afetar o desempenho geral.

Considerações de atualização e reversão de passagem-leitura

Há certas considerações de atualização e reversão que você deve saber antes de atualizar para uma versão do ONTAP que suporta passagem-leitura ou antes de reverter para uma versão que não suporta passagem-leitura.

A atualizar

Depois que todos os nós são atualizados para uma versão do ONTAP que suporte a passagem-leitura FPolicy, o cluster é capaz de usar a funcionalidade de leitura de passagem; no entanto, a leitura de passagem é desativada por padrão nas configurações FPolicy existentes. Para usar a leitura de passagem em configurações FPolicy existentes, você deve desativar a política FPolicy e modificar a configuração e, em seguida, reativar a configuração.

Reverter

Antes de reverter para uma versão do ONTAP que não suporte a passagem-leitura de FPolicy, você deve atender às seguintes condições:

- Desative todas as políticas usando passthrough-read e, em seguida, modifique as configurações afetadas para que elas não usem passthrough-read.
- Desative a funcionalidade FPolicy no cluster desativando todas as políticas FPolicy no cluster.

Antes de reverter para uma versão do ONTAP que não ofereça suporte a armazenamentos persistentes, certifique-se de que nenhuma das diretivas FPolicy tenha um armazenamento persistente configurado. Se um armazenamento persistente estiver configurado, a reversão falhará.

Quais são os passos para configurar uma configuração FPolicy

Antes que o FPolicy possa monitorar o acesso a arquivos, uma configuração FPolicy deve ser criada e ativada na máquina virtual de storage (SVM) para a qual os serviços FPolicy são necessários.

As etapas para configurar e habilitar uma configuração FPolicy no SVM são as seguintes:

1. Crie um mecanismo externo FPolicy.

   O mecanismo externo FPolicy identifica os servidores FPolicy externos (servidores FPolicy) que estão associados a uma configuração FPolicy específica. Se o mecanismo FPolicy "'nativo" interno for usado para criar uma configuração nativa de bloqueio de arquivos, você não precisará criar um mecanismo externo FPolicy.

   Começando com ONTAP 9.15,1, você pode usar o `protobuf` formato do motor. Quando definido como `protobuf`, as mensagens de notificação são codificadas de forma binária usando o Google Protobuf. Antes de definir o formato do mecanismo como `protobuf`, certifique-se de que o servidor FPolicy também suporta `protobuf` a desserialização. Para obter mais informações, consulte "Planeie a configuração do motor externo FPolicy"

2. Criar um evento FPolicy.

   Um evento FPolicy descreve o que a política FPolicy deve monitorar. Os eventos consistem em protocolos e operações de arquivo a serem monitoradas e podem conter uma lista de filtros. Eventos Use filtros para restringir a lista de eventos monitorados para os quais o mecanismo externo FPolicy deve enviar notificações. Os eventos também especificam se a diretiva monitora as operações de volume.

3. Crie um armazenamento persistente FPolicy (opcional).

   A partir do ONTAP 9.14,1, o FPolicy permite que você configure "armazenamentos persistentes"para capturar eventos de acesso a arquivos para políticas assíncronas não obrigatórias no SVM. Configurações síncronas (obrigatórias ou não obrigatórias) e assíncronas obrigatórias não são suportadas.

   Armazenamentos persistentes podem ajudar a desacoplar o processamento de e/S do cliente do processamento de notificações FPolicy para reduzir a latência do cliente.

   A partir do ONTAP 9.15,1, a configuração de armazenamento persistente do FPolicy é simplificada. O `persistent-store-create` comando automatiza a criação de volume para o SVM e configura o volume para o armazenamento persistente.

4. Crie uma política FPolicy.

   A política FPolicy é responsável por associar, com o escopo apropriado, o conjunto de eventos que

precisam ser monitorados e para qual das notificações de eventos monitorados deve ser enviado para o servidor FPolicy designado (ou para o mecanismo nativo se nenhum servidor FPolicy estiver configurado). A política também define se o servidor FPolicy tem acesso privilegiado aos dados para os quais recebe notificações. Um servidor FPolicy precisa de acesso privilegiado se o servidor precisar acessar os dados. Os casos de uso típicos em que o acesso privilegiado é necessário incluem bloqueio de arquivos, gerenciamento de cotas e gerenciamento de storage hierárquico. A política é onde você especifica se a configuração para essa política usa um servidor FPolicy ou o servidor FPolicy interno "'nativo".

Uma política especifica se a triagem é obrigatória. Se a triagem for obrigatória e todos os servidores FPolicy estiverem inativos ou se nenhuma resposta for recebida dos servidores FPolicy dentro de um período de tempo limite definido, o acesso ao arquivo será negado.

Os limites de uma política são o SVM. Uma política não pode se aplicar a mais de um SVM. No entanto, um SVM específico pode ter várias políticas de FPolicy, cada uma com a mesma combinação ou diferente de configurações de escopo, evento e servidor externo.

5. Configure o escopo da política.

   O escopo da FPolicy determina quais volumes, compartilhamentos ou políticas de exportação a política atua ou exclui do monitoramento. Um escopo também determina quais extensões de arquivo devem ser incluídas ou excluídas do monitoramento FPolicy.

   Excluir listas têm precedência sobre incluir listas.

6. Ative a política FPolicy.

   Quando a política está ativada, os canais de controle e, opcionalmente, os canais de dados privilegiados são conetados. O processo de FPolicy nos nós nos quais o SVM participa começa a monitorar o acesso a arquivos e pastas e, para eventos que correspondam aos critérios configurados, envia notificações para os servidores FPolicy (ou para o mecanismo nativo se nenhum servidor FPolicy estiver configurado).

Se a política usar bloqueio de arquivos nativo, um mecanismo externo não será configurado ou associado à política.

Planeie a configuração do motor externo FPolicy

Planeie a configuração do motor externo FPolicy

Antes de configurar o mecanismo externo FPolicy, você deve entender o que significa criar um mecanismo externo e quais parâmetros de configuração estão disponíveis. Essas informações ajudam você a determinar quais valores definir para cada parâmetro.

Informações que são definidas ao criar o mecanismo externo FPolicy

A configuração do mecanismo externo define as informações que o FPolicy precisa para fazer e gerenciar conexões com os servidores FPolicy externos, incluindo o seguinte:

- Nome do SVM
- Nome do motor
- Os endereços IP dos servidores FPolicy primário e secundário e o número da porta TCP a serem usados ao fazer a conexão com os servidores FPolicy

- Se o tipo de motor é assíncrono ou síncrono
- Se o formato do motor é `xml` ou `protobuf`

  Começando com ONTAP 9.15,1, você pode usar o `protobuf` formato do motor. Quando definido como `protobuf`, as mensagens de notificação são codificadas de forma binária usando o Google Protobuf. Antes de definir o formato do mecanismo como `protobuf`, certifique-se de que o servidor FPolicy também suporta `protobuf` a desserialização.

  Uma vez que o formato protobuf é suportado a partir de ONTAP 9.15,1, você deve considerar o formato externo do motor antes de reverter para uma versão anterior do ONTAP. Se você reverter para uma versão anterior do ONTAP 9.15,1, trabalhe com seu parceiro FPolicy para:

  - Altere cada formato do motor de `protobuf` para `xml`
  - Elimine os motores com um formato de motor de `protobuf`
- Como autenticar a conexão entre o nó e o servidor FPolicy

  Se você optar por configurar a autenticação SSL mútua, você também deve configurar parâmetros que fornecem informações de certificado SSL.

- Como gerir a ligação utilizando várias definições avançadas de privilégios

  Isso inclui parâmetros que definem coisas como valores de tempo limite, valores de repetição, valores de keep-alive, valores máximos de solicitação, valores de tamanho de buffer enviados e recebidos e valores de tempo limite da sessão.

O `vserver fpolicy policy external-engine create` comando é usado para criar um mecanismo externo FPolicy.

Quais são os parâmetros básicos do motor externo

Você pode usar a seguinte tabela de parâmetros básicos de configuração do FPolicy para ajudá-lo a Planejar sua configuração:

Tipo de informação	Opção
SVM Especifica o nome do SVM que você deseja associar a esse mecanismo externo. Cada configuração de FPolicy é definida em um único SVM. O mecanismo externo, o evento de política, o escopo da política e a política que se combinam para criar uma configuração de política FPolicy devem estar associados ao mesmo SVM.	`-vserver vserver_name`

Nome do motor Especifica o nome a ser atribuído à configuração externa do motor. Você deve especificar o nome do mecanismo externo mais tarde quando criar a política FPolicy. Isto associa o motor externo à política. O nome pode ter até 256 carateres. O nome deve ter até 200 carateres se estiver configurando o nome do mecanismo externo em uma configuração de recuperação de desastres do MetroCluster ou SVM. O nome pode conter qualquer combinação dos seguintes carateres de intervalo ASCII: • `a` através `z` • `A` através `Z` • `0` através `9` • "»_", "-", `and` "»."	`-engine-name engine_name`
Servidores FPolicy primários Especifica os servidores FPolicy primários para os quais o nó envia notificações para uma determinada política FPolicy. O valor é especificado como uma lista delimitada por vírgulas de endereços IP. Se mais de um endereço IP de servidor primário for especificado, cada nó no qual o SVM participa criará uma conexão de controle para cada servidor FPolicy primário especificado no momento em que a diretiva é ativada. Se você configurar vários servidores FPolicy primários, as notificações serão enviadas para os servidores FPolicy de forma redonda. Se o mecanismo externo for usado em uma configuração de recuperação de desastres do MetroCluster ou SVM, você deverá especificar os endereços IP dos servidores FPolicy no local de origem como servidores primários. Os endereços IP dos servidores FPolicy no local de destino devem ser especificados como servidores secundários.	`-primary-servers IP_address,...`
Número da porta Especifica o número da porta do serviço FPolicy.	`-port integer`

Servidores FPolicy secundários Especifica os servidores FPolicy secundários para os quais enviar eventos de acesso a arquivos para uma determinada política FPolicy. O valor é especificado como uma lista delimitada por vírgulas de endereços IP. Os servidores secundários são utilizados apenas quando nenhum dos servidores primários é alcançável. As conexões com servidores secundários são estabelecidas quando a diretiva está ativada, mas as notificações são enviadas para servidores secundários somente se nenhum dos servidores primários estiver acessível. Se você configurar vários servidores secundários, as notificações serão enviadas para os servidores FPolicy de forma redonda.	`-secondary-servers IP_address,...`
Tipo de motor externo Especifica se o mecanismo externo opera no modo síncrono ou assíncrono. Por padrão, o FPolicy opera no modo síncrono. Quando definido como `synchronous`, o processamento de solicitação de arquivo envia uma notificação para o servidor FPolicy, mas depois não continua até receber uma resposta do servidor FPolicy. Nesse ponto, o fluxo de solicitação continua ou o processamento resulta em negação, dependendo se a resposta do servidor FPolicy permite a ação solicitada. Quando definido como `asynchronous`, o processamento de solicitação de arquivo envia uma notificação para o servidor FPolicy e, em seguida, continua.	`-extern-engine-type external_engine_type` O valor para este parâmetro pode ser um dos seguintes: • `synchronous` • `asynchronous`
Formato externo do motor Especifique se o formato do mecanismo externo é xml ou protobuf. Começando com ONTAP 9.15,1, você pode usar o formato do mecanismo protobuf. Quando definido como protobuf, as mensagens de notificação são codificadas em forma binária usando o Google Protobuf. Antes de definir o formato do motor para protobuf, certifique-se de que o servidor FPolicy também suporta a desserialização de protobuf.	`- extern-engine-format` {`protobuf` ou `xml`

Opção SSL para comunicação com o servidor FPolicy Especifica a opção SSL para comunicação com o servidor FPolicy. Este é um parâmetro obrigatório. Você pode escolher uma das opções com base nas seguintes informações: • Quando definido como `no-auth`, não ocorre autenticação. O link de comunicação é estabelecido através do TCP. • Quando definido como `server-auth`, o SVM autentica o servidor FPolicy usando autenticação de servidor SSL. • Quando definido como `mutual-auth`, a autenticação mútua ocorre entre o SVM e o servidor FPolicy; o SVM autentica o servidor FPolicy e o servidor FPolicy autentica o SVM. Se você optar por configurar a autenticação SSL mútua, também deverá configurar os `-certificate-common-name` parâmetros , `-certificate-serial` e `-certifcate-ca` .	`-ssl-option` {`no-auth`
`server-auth`	`mutual-auth`Selecione
Certificado FQDN ou nome comum personalizado Especifica o nome do certificado usado se a autenticação SSL entre o SVM e o servidor FPolicy estiver configurada. Você pode especificar o nome do certificado como um FQDN ou como um nome comum personalizado. Se você especificar `mutual-auth` para o `-ssl-option` parâmetro, será necessário especificar um valor para o `-certificate-common-name` parâmetro.	`-certificate-common -name` `text`
Número de série do certificado Especifica o número de série do certificado usado para autenticação se a autenticação SSL entre o SVM e o servidor FPolicy estiver configurada. Se você especificar `mutual-auth` para o `-ssl-option` parâmetro, será necessário especificar um valor para o `-certificate-serial` parâmetro.	`-certificate-serial` `text`
Autoridade de certificação Especifica o nome da CA do certificado usado para autenticação se a autenticação SSL entre o SVM e o servidor FPolicy estiver configurada. Se você especificar `mutual-auth` para o `-ssl-option` parâmetro, será necessário especificar um valor para o `-certificate-ca` parâmetro.	`-certificate-ca` `text`

Quais são as opções avançadas do motor externo

Você pode usar a seguinte tabela de parâmetros avançados de configuração FPolicy à medida que planeja personalizar sua configuração com parâmetros avançados. Você usa esses parâmetros para modificar o comportamento de comunicação entre os nós de cluster e os servidores FPolicy:

Tipo de informação	Opção
Tempo limite para cancelar uma solicitação Especifica o intervalo de tempo em horas (`h`), (`m`minutos) ou segundos (`s`) que o nó espera por uma resposta do servidor FPolicy. Se o intervalo de tempo limite passar, o nó envia uma solicitação de cancelamento para o servidor FPolicy. O nó então envia a notificação para um servidor FPolicy alternativo. Esse tempo limite ajuda a lidar com um servidor FPolicy que não está respondendo, o que pode melhorar a resposta do cliente SMB/NFS. Além disso, cancelar solicitações após um período de tempo limite pode ajudar a liberar recursos do sistema porque a solicitação de notificação é movida de um servidor FPolicy inativo/ruim para um servidor FPolicy alternativo. O intervalo para este valor é `0` através `100`de . Se o valor estiver definido como `0`, a opção será desativada e as mensagens de solicitação de cancelamento não serão enviadas para o servidor FPolicy. A predefinição é `20s`.	`-reqs-cancel-timeout integer`[h
m	s]
Tempo limite para abortar uma solicitação Especifica o tempo limite em horas (`h`), (`m`minutos) ou segundos (`s`) para abortar uma solicitação. O intervalo para este valor é `0` através `200`de .	`-reqs-abort-timeout ` `integer`[h
m	s]
Intervalo para envio de solicitações de status Especifica o intervalo em horas (`h`), minutos (`m`) ou segundos (`s`) após o qual uma solicitação de status é enviada ao servidor FPolicy. O intervalo para este valor é `0` através `50`de . Se o valor estiver definido como `0`, a opção será desativada e as mensagens de solicitação de status não serão enviadas ao servidor FPolicy. A predefinição é `10s`.	`-status-req-interval integer`[h
m	s]

Máximo de solicitações pendentes no servidor FPolicy Especifica o número máximo de solicitações pendentes que podem ser enfileiradas no servidor FPolicy. O intervalo para este valor é `1` através `10000`de . A predefinição é `500`.	`-max-server-reqs integer`
Tempo limite para desconetar um servidor FPolicy não responsivo Especifica o intervalo de tempo em horas (`h`), (`m`minutos) ou segundos (`s`) após o qual a conexão com o servidor FPolicy é encerrada. A conexão é encerrada após o período de tempo limite somente se a fila do servidor FPolicy contiver o máximo de solicitações permitidas e nenhuma resposta for recebida dentro do período de tempo limite. O número máximo permitido de solicitações é `50` (o padrão) ou o número especificado pelo `max-server-reqs-` parâmetro. O intervalo para este valor é `1` através `100`de . A predefinição é `60s`.	`-server-progress -timeout integer`[h
m	s]
Intervalo para enviar mensagens keep-alive para o servidor FPolicy Especifica o intervalo de tempo em horas (`h`), (`m`minutos) ou segundos (`s`) no qual as mensagens keep-alive são enviadas ao servidor FPolicy. As mensagens keep-alive detetam conexões semi-abertas. O intervalo para este valor é `10` através `600`de . Se o valor estiver definido como `0`, a opção será desativada e as mensagens de manutenção em tempo real serão impedidas de serem enviadas para os servidores FPolicy. A predefinição é `120s`.	`-keep-alive-interval- integer`[h
m	s]
Máximo de tentativas de reconexão Especifica o número máximo de vezes que o SVM tenta se reconetar ao servidor FPolicy depois que a conexão foi interrompida. O intervalo para este valor é `0` através `20`de . A predefinição é `5`.	`-max-connection-retries integer`

Receive buffer size Especifica o tamanho do buffer de receção do soquete conetado para o servidor FPolicy. O valor padrão é definido como 256 kilobytes (Kb). Quando o valor é definido como 0, o tamanho do buffer de receção é definido para um valor definido pelo sistema. Por exemplo, se o tamanho padrão do buffer de recebimento do soquete for de 65536 bytes, definindo o valor ajustável como 0, o tamanho do buffer do soquete será definido como 65536 bytes. Você pode usar qualquer valor não padrão para definir o tamanho (em bytes) do buffer de recebimento.	`-recv-buffer-size integer`
Enviar tamanho do buffer Especifica o tamanho do buffer de envio do soquete conetado para o servidor FPolicy. O valor padrão é definido como 256 kilobytes (Kb). Quando o valor é definido como 0, o tamanho do buffer de envio é definido para um valor definido pelo sistema. Por exemplo, se o tamanho padrão do buffer de envio do soquete for definido como 65536 bytes, definindo o valor ajustável como 0, o tamanho do buffer do soquete será definido como 65536 bytes. Você pode usar qualquer valor não padrão para definir o tamanho (em bytes) do buffer de envio.	`-send-buffer-size integer`
Tempo limite para purgar um Session ID durante a reconexão Especifica o intervalo em horas (`h`), minutos (`m`) ou segundos (`s`) após o qual um novo Session ID é enviado ao servidor FPolicy durante tentativas de reconexão. Se a conexão entre o controlador de armazenamento e o servidor FPolicy for encerrada e a nova conexão for feita dentro do `-session-timeout` intervalo, o Session ID antigo será enviado para o servidor FPolicy para que ele possa enviar respostas para notificações antigas. O valor padrão é definido para 10 segundos.	`-session-timeout integer[ m][integers]`

Informações adicionais sobre a configuração de mecanismos externos FPolicy para usar conexões autenticadas SSL

Você precisa saber algumas informações adicionais se quiser configurar o mecanismo externo FPolicy para usar SSL ao se conetar a servidores FPolicy.

Autenticação de servidor SSL

Se você optar por configurar o mecanismo externo FPolicy para autenticação de servidor SSL, antes de criar o mecanismo externo, você deverá instalar o certificado público da autoridade de certificação (CA) que assinou

o certificado do servidor FPolicy.

Autenticação mútua

Se você configurar mecanismos externos do FPolicy para usar a autenticação mútua SSL ao conetar LIFs de dados da máquina virtual de armazenamento (SVM) a servidores FPolicy externos, antes de criar o mecanismo externo, você deverá instalar o certificado público da CA que assinou o certificado do servidor FPolicy juntamente com o certificado público e o arquivo chave para autenticação do SVM. Não exclua este certificado enquanto nenhuma política FPolicy estiver usando o certificado instalado.

Se o certificado for excluído enquanto o FPolicy estiver usando-o para autenticação mútua ao se conetar a um servidor FPolicy externo, não será possível reativar uma política FPolicy desativada que use esse certificado. A política FPolicy não pode ser reativada nessa situação mesmo que um novo certificado com as mesmas configurações seja criado e instalado no SVM.

Se o certificado tiver sido excluído, você precisará instalar um novo certificado, criar novos mecanismos externos FPolicy que usam o novo certificado e associar os novos mecanismos externos à política FPolicy que você deseja reativar modificando a política FPolicy.

Instale certificados para SSL

O certificado público da CA que é usado para assinar o certificado do servidor FPolicy é instalado usando o `security certificate install` comando com o `-type` parâmetro definido como `client-ca`. A chave privada e o certificado público necessários para a autenticação do SVM são instalados usando o `security certificate install` comando com o `-type` parâmetro definido como `server`.

Os certificados não são replicados nas relações de recuperação de desastres do SVM com uma configuração que não preserve ID

Os certificados de segurança usados para autenticação SSL ao fazer conexões com servidores FPolicy não são replicados para destinos de recuperação de desastres SVM com configurações que não preservem ID. Embora a configuração do mecanismo externo FPolicy na SVM seja replicada, os certificados de segurança não são replicados. Tem de instalar manualmente os certificados de segurança no destino.

Quando você configura a relação de recuperação de desastres SVM, o valor selecionado para a `-identity-preserve` opção `snapmirror create` do comando determina os detalhes de configuração replicados no SVM de destino.

Se você definir `-identity-preserve` a opção como `true` (ID-Preserve), todos os detalhes de configuração do FPolicy serão replicados, incluindo as informações do certificado de segurança. Só tem de instalar os certificados de segurança no destino se definir a opção como `false` (non-ID-Preserve).

Restrições para mecanismos externos de FPolicy com escopo de cluster com configurações de recuperação de desastres MetroCluster e SVM

Você pode criar um mecanismo externo FPolicy com escopo de cluster atribuindo a máquina virtual de armazenamento de cluster (SVM) ao mecanismo externo. No entanto, ao criar um mecanismo externo com escopo de cluster em uma configuração de recuperação de desastres MetroCluster ou SVM, há certas restrições ao escolher o método de autenticação usado pelo SVM para comunicação externa com o servidor

FPolicy.

Há três opções de autenticação que você pode escolher ao criar servidores FPolicy externos: sem autenticação, autenticação de servidor SSL e autenticação mútua SSL. Embora não haja restrições ao escolher a opção de autenticação se o servidor FPolicy externo for atribuído a um SVM de dados, há restrições ao criar um mecanismo externo FPolicy com escopo de cluster:

Configuração	Permitido?
Recuperação de desastres MetroCluster ou SVM e um mecanismo externo FPolicy com escopo de cluster sem autenticação (SSL não está configurado)	Sim
Recuperação de desastres MetroCluster ou SVM e um mecanismo externo FPolicy com escopo de cluster com autenticação mútua SSL ou SSL	Não

- Se houver um mecanismo externo FPolicy com escopo de cluster e autenticação SSL e você quiser criar uma configuração de recuperação de desastres do MetroCluster ou SVM, modifique esse mecanismo externo para não usar autenticação ou remover o mecanismo externo antes de criar a configuração de recuperação de desastres do MetroCluster ou SVM.
- Se a configuração de recuperação de desastres do MetroCluster ou SVM já existir, o ONTAP impede que você crie um mecanismo externo FPolicy com escopo de cluster com autenticação SSL.

Preencha a folha de cálculo de configuração do motor externo FPolicy

Você pode usar esta Planilha para Registrar os valores que você precisa durante o processo de configuração do mecanismo externo FPolicy. Se um valor de parâmetro for necessário, você precisará determinar qual valor usar para esses parâmetros antes de configurar o mecanismo externo.

Informações para uma configuração externa básica do motor

Você deve Registrar se deseja incluir cada configuração de parâmetro na configuração do mecanismo externo e, em seguida, Registrar o valor para os parâmetros que deseja incluir.

Tipo de informação	Obrigatório	Incluir	Seus valores
Nome da máquina virtual de storage (SVM)	Sim	Sim	
Nome do motor	Sim	Sim	
Servidores FPolicy primários	Sim	Sim	
Número da porta	Sim	Sim	
Servidores FPolicy secundários	Não		
Tipo de motor externo	Não		

Opção SSL para comunicação com servidor FPolicy externo	Sim	Sim	
Certificado FQDN ou nome comum personalizado	Não		
Número de série do certificado	Não		
Autoridade de certificação	Não		

Informações para parâmetros externos avançados do motor

Para configurar um motor externo com parâmetros avançados, tem de introduzir o comando de configuração no modo de privilégio avançado.

Tipo de informação	Obrigatório	Incluir	Seus valores
Tempo limite para cancelar uma solicitação	Não		
Tempo limite para abortar uma solicitação	Não		
Intervalo para envio de solicitações de status	Não		
Máximo de solicitações pendentes no servidor FPolicy	Não		
Tempo limite para desconetar um servidor FPolicy não responsivo	Não		
Intervalo para enviar mensagens keep-alive para o servidor FPolicy	Não		
Máximo de tentativas de reconexão	Não		
Receber tamanho do buffer	Não		
Enviar tamanho do buffer	Não		
Tempo limite para purgar um Session ID durante a reconexão	Não		

Planeje a configuração do evento FPolicy

Planeje a visão geral da configuração de eventos FPolicy

Antes de configurar eventos FPolicy, você deve entender o que significa criar um evento FPolicy. Você deve determinar quais protocolos deseja que o evento monitore, quais eventos monitorar e quais filtros de eventos usar. Essas informações ajudam a Planejar os valores que você deseja definir.

O que significa criar um evento FPolicy

Criar o evento FPolicy significa definir as informações que o processo FPolicy precisa para determinar quais operações de acesso a arquivos monitorar e para quais notificações de eventos monitorados devem ser enviadas para o servidor FPolicy externo. A configuração do evento FPolicy define as seguintes informações de configuração:

- Nome da máquina virtual de storage (SVM)
- Nome do evento
- Quais protocolos monitorar

  O FPolicy pode monitorar SMB, NFSv3, NFSv4 e, a partir de operações de acesso a arquivos ONTAP 9.15,1, NFSv4,1.

- Quais operações de arquivo monitorar

  Nem todas as operações de arquivo são válidas para cada protocolo.

- Quais filtros de arquivo configurar

  Apenas determinadas combinações de operações de arquivo e filtros são válidas. Cada protocolo tem seu próprio conjunto de combinações suportadas.

- Se deve monitorar a montagem de volume e desmontar operações

> Existe uma dependência com três dos parâmetros (`-protocol`, `-file-operations`, `-filters`). As seguintes combinações são válidas para os três parâmetros:
>
> - Pode especificar os `-protocol` parâmetros e. `-file-operations`
> - Você pode especificar todos os três parâmetros.
> - Não é possível especificar nenhum dos parâmetros.

O que contém a configuração do evento FPolicy

Você pode usar a seguinte lista de parâmetros de configuração de eventos FPolicy disponíveis para ajudá-lo a Planejar sua configuração:

Tipo de informação	Opção

SVM Especifica o nome do SVM que você deseja associar a este evento FPolicy. Cada configuração de FPolicy é definida em um único SVM. O mecanismo externo, o evento de política, o escopo da política e a política que se combinam para criar uma configuração de política FPolicy devem estar associados ao mesmo SVM.	`-vserver vserver_name`
Nome do evento Especifica o nome a ser atribuído ao evento FPolicy. Quando você cria a política FPolicy, você associa o evento FPolicy à política usando o nome do evento. O nome pode ter até 256 carateres. O nome deve ter até 200 carateres se o evento for configurado em uma configuração de recuperação de desastres do MetroCluster ou SVM. O nome pode conter qualquer combinação dos seguintes carateres de intervalo ASCII: • `a` através `z` • `A` através `Z` • `0` através `9` • "`_`,"`-`", `and` ".».	`-event-name event_name`
Protocolo Especifica qual protocolo configurar para o evento FPolicy. A lista para `-protocol` pode incluir um dos seguintes valores: • `cifs` • `nfsv3` • `nfsv4` Se você especificar `-protocol`, então você deve especificar um valor válido no `-file-operations` parâmetro. À medida que a versão do protocolo muda, os valores válidos podem mudar. A partir do ONTAP 9.15,1, o NFSv4 permite capturar eventos NFSv4,0 e NFSv4,1.	`-protocol protocol`

Operações de arquivo Especifica a lista de operações de arquivo para o evento FPolicy. O evento verifica as operações especificadas nesta lista a partir de todas as solicitações de cliente usando o protocolo especificado no `-protocol` parâmetro. Você pode listar uma ou mais operações de arquivo usando uma lista delimitada por vírgulas. A lista para `-file-operations` pode incluir um ou mais dos seguintes valores: • `close` para operações de fechamento de arquivo • `create` para operações de criação de arquivo • `create-dir` para operações de criação de diretório • `delete` para operações de exclusão de arquivos • `delete_dir` para operações de exclusão de diretório • `getattr` para obter operações de atributo • `link` para operações de link • `lookup` para operações de pesquisa • `open` para operações de arquivo aberto • `read` para operações de leitura de arquivos • `write` para operações de gravação de arquivos • `rename` para operações de renomeação de arquivo • `rename_dir` para operações de renomeação de diretório • `setattr` para definir operações de atributo • `symlink` para operações de link simbólico Se especificar `-file-operations`, deve especificar um protocolo válido no `-protocol` parâmetro.	`-file-operations file_operations,...`

Filtros Especifica a lista de filtros para uma determinada operação de arquivo para o protocolo especificado. Os valores no `-filters` parâmetro são usados para filtrar as solicitações do cliente. A lista pode incluir um ou mais dos seguintes itens: Se você especificar o `-filters` parâmetro, também deverá especificar valores válidos para os `-file-operations` parâmetros e. `-protocol` • `monitor-ads` opção para filtrar a solicitação do cliente para fluxo de dados alternativo. • `close-with-modification` opção para filtrar a solicitação do cliente para fechar com modificação. • `close-without-modification` opção para filtrar a solicitação do cliente para fechar sem modificação. • `first-read` opção para filtrar a solicitação do cliente para primeira leitura. • `first-write` opção para filtrar a solicitação do cliente para a primeira gravação. • `offline-bit` opção para filtrar a solicitação do cliente para o conjunto de bits off-line. A configuração desse filtro resulta no servidor FPolicy recebendo notificações somente quando os arquivos off-line são acessados. • `open-with-delete-intent` opção para filtrar a solicitação do cliente para abrir com delete intent. A configuração desse filtro faz com que o servidor FPolicy receba notificações somente quando for feita uma tentativa de abrir um arquivo com a intenção de excluí-lo. Isso é usado por sistemas de arquivos quando o `FILE_DELETE_ON_CLOSE` sinalizador é especificado. • `open-with-write-intent` opção para filtrar a solicitação do cliente para aberta com intenção de gravação. A configuração desse filtro faz com que o servidor FPolicy receba notificações somente quando for feita uma tentativa de abrir um arquivo com a intenção de escrever algo nele. • `write-with-size-change` opção para filtrar a solicitação do cliente para gravação com alteração de tamanho. • `setattr-with-owner-change` opção para filtrar as solicitações de setattr do cliente para alterar o proprietário de um arquivo ou de um diretório. • `setattr-with-group-change` opção para filtrar as solicitações de setattr do cliente para alterar o grupo de um arquivo ou um diretório. `setattr-with-sacl-change` Opção para filtrar as solicitações de setattr do cliente para alterar o SACL em um arquivo ou diretório. Este filtro está disponível apenas para os protocolos SMB e NFSv4.	`-filters filter, ...`

É a operação de volume necessária Especifica se o monitoramento é necessário para operações de montagem de volume e desmontagem. A predefinição é `false`.	`-volume-operation {true`
`false`Selecione `-filters filter, ...	*FPolicy Acesso negado notificações* A partir do ONTAP 9.13,1, os usuários podem receber notificações para operações de arquivos com falha devido à falta de permissões. Essas notificações são valiosas para segurança, proteção contra ransomware e governança. As notificações serão geradas para a operação do arquivo falhou devido à falta de permissão, o que inclui: • Falhas devido a permissões NTFS. • Falhas devido a bits de modo Unix. • Falhas devido a ACLs NFSv4.
`-monitor-fileop-failure {true Quando esse filtro é especificado, as operações do diretório não são monitoradas.	`false`Selecione

Operação de arquivo suportada e combinações de filtro que o FPolicy pode monitorar para SMB

Ao configurar seu evento FPolicy, você precisa estar ciente de que apenas determinadas combinações de operações de arquivo e filtros são suportadas para monitorar operações de acesso a arquivos SMB.

A lista de combinações de filtros e operação de arquivos compatíveis para monitoramento FPolicy de eventos de acesso a arquivos SMB é fornecida na tabela a seguir:

Operações de arquivos compatíveis	Filtros suportados
fechar	monitor-ads, off-line-bit, close-com-modificação, close-sem-modificação, close-com-leitura, exclude-diretório
criar	monitor-anúncios, off-line-bit

criar_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
eliminar	monitor-anúncios, off-line-bit
delete_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
getattr	offline-bit, exclude-dir
abrir	monitore anúncios, off-line-bit, open-with-delete-intent, open-with-write-intent, exclude-dir
leia	monitore anúncios, off-line-bit, primeira leitura
escreva	monitore anúncios, off-line-bit, primeira gravação, write-with-size-change
mudar o nome	monitor-anúncios, off-line-bit
rename_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
ajuste	monitor-ads, off-line-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_time_change

A partir do ONTAP 9.13,1, os usuários podem receber notificações para operações de arquivos com falha devido à falta de permissões. A lista de combinações de filtro e operação de arquivo negado de acesso com suporte para monitoramento FPolicy de eventos de acesso a arquivos SMB é fornecida na tabela a seguir:

Acesso suportado operação de arquivo negado	Filtros suportados
abrir	NA

Operação de arquivo suportada e combinações de filtro que o FPolicy pode monitorar para NFSv3

Ao configurar seu evento FPolicy, você precisa estar ciente de que apenas certas combinações de operações de arquivo e filtros são suportadas para monitorar operações de acesso a arquivos NFSv3.

A lista de combinações de filtros e operação de arquivos compatíveis para monitoramento FPolicy de eventos de acesso a arquivos NFSv3 é fornecida na seguinte tabela:

Operações de arquivos compatíveis	Filtros suportados
criar	bit offline

criar_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
eliminar	bit offline
delete_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
link	bit offline
pesquisa	offline-bit, exclude-dir
leia	offline-bit, primeira leitura
escreva	offline-bit, primeira gravação, write-with-size-change
mudar o nome	bit offline
rename_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
ajuste	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
link simbólico	bit offline

A partir do ONTAP 9.13,1, os usuários podem receber notificações para operações de arquivos com falha devido à falta de permissões. A lista de combinações de filtro e operação de arquivo negado de acesso suportado para monitoramento FPolicy de eventos de acesso a arquivos NFSv3 é fornecida na seguinte tabela:

Acesso suportado operação de arquivo negado	Filtros suportados
acesso	NA
criar	NA
criar_dir	NA
eliminar	NA
delete_dir	NA
link	NA
leia	NA

mudar o nome	NA
rename_dir	NA
ajuste	NA
escreva	NA

Operação de arquivo suportada e combinações de filtro que o FPolicy pode monitorar para NFSv4

Ao configurar seu evento FPolicy, você precisa estar ciente de que apenas certas combinações de operações de arquivo e filtros são suportadas para monitorar operações de acesso a arquivos NFSv4.

A partir do ONTAP 9.15,1, o FPolicy suporta o protocolo NFSv4,1.

A lista de combinações de filtros e operação de arquivos compatíveis para monitoramento FPolicy de eventos de acesso a arquivos NFSv4 ou NFSv4,1 é fornecida na seguinte tabela:

Operações de arquivos compatíveis	Filtros suportados
fechar	offline-bit, exclude-directory
criar	bit offline
criar_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
eliminar	bit offline
delete_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
getattr	offline-bit, exclude-directory
link	bit offline
pesquisa	offline-bit, exclude-directory
abrir	offline-bit, exclude-directory
leia	offline-bit, primeira leitura
escreva	offline-bit, primeira gravação, write-with-size-change
mudar o nome	bit offline

rename_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
ajuste	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_time_change, setattr_change, setattr_time_change, setattr_change
link simbólico	bit offline

A partir do ONTAP 9.13,1, os usuários podem receber notificações para operações de arquivos com falha devido à falta de permissões. A lista de combinações de filtro e operação de arquivo negado de acesso com suporte para monitoramento FPolicy de eventos de acesso a arquivos NFSv4 ou NFSv4,1 é fornecida na tabela a seguir:

Acesso suportado operação de arquivo negado	Filtros suportados
acesso	NA
criar	NA
criar_dir	NA
eliminar	NA
delete_dir	NA
link	NA
abrir	NA
leia	NA
mudar o nome	NA
rename_dir	NA
ajuste	NA
escreva	NA

Preencha a Planilha de configuração de evento FPolicy

Você pode usar essa Planilha para Registrar os valores necessários durante o processo de configuração de evento FPolicy. Se um valor de parâmetro for necessário, você

precisará determinar qual valor usar para esses parâmetros antes de configurar o evento FPolicy.

Você deve Registrar se deseja incluir cada configuração de parâmetro na configuração do evento FPolicy e, em seguida, Registrar o valor para os parâmetros que deseja incluir.

Tipo de informação	Obrigatório	Incluir	Seus valores
Nome da máquina virtual de storage (SVM)	Sim	Sim	
Nome do evento	Sim	Sim	
Protocolo	Não		
Operações de arquivos	Não		
Filtros	Não		
Operação de volume	Não		
Acesse eventos negados (suporte a partir de ONTAP 9.13)	Não		

Planeie a configuração da política FPolicy

Planeje a visão geral da configuração da política FPolicy

Antes de configurar a política FPolicy, você deve entender quais parâmetros são necessários ao criar a política, bem como por que você pode querer configurar determinados parâmetros opcionais. Essas informações ajudam você a determinar quais valores definir para cada parâmetro.

Ao criar uma política FPolicy, você associa a política ao seguinte:

- A máquina virtual de storage (SVM)
- Um ou mais eventos FPolicy
- Um motor externo FPolicy

Você também pode configurar várias configurações de política opcionais.

O que contém a configuração da política FPolicy

Você pode usar a seguinte lista de parâmetros opcionais e de política FPolicy disponíveis para ajudá-lo a Planejar sua configuração:

Tipo de informação	Opção	Obrigatório	Padrão

Nome da SVM Especifica o nome do SVM no qual você deseja criar uma política de FPolicy.	`-vserver vserver_name`	Sim	Nenhum
Nome da política Especifica o nome da política FPolicy. O nome pode ter até 256 carateres. O nome deve ter até 200 carateres se a diretiva estiver configurada em uma configuração de recuperação de desastres do MetroCluster ou SVM. O nome pode conter qualquer combinação dos seguintes carateres de intervalo ASCII: • `a` através `z` • `A` através `Z` • `0` através `9` • "»_", "`-`", `and` "»."	`-policy-name policy_name`	Sim	Nenhum
Nomes de eventos Especifica uma lista delimitada por vírgulas de eventos a serem associados à política FPolicy. • Você pode associar mais de um evento a uma política. • Um evento é específico de um protocolo. • Você pode usar uma única política para monitorar eventos de acesso a arquivos para mais de um protocolo, criando um evento para cada protocolo que você deseja que a diretiva monitore e associando os eventos à política. • Os eventos já devem existir.	`-events event_name, ...`	Sim	Nenhum

Armazenamento persistente A partir do ONTAP 9.14,1, este parâmetro especifica o armazenamento persistente para capturar eventos de acesso a arquivos para políticas assíncronas não obrigatórias no SVM.	`-persistent -store persistent_store_name`	Não	Nenhum
Nome externo do motor Especifica o nome do mecanismo externo a ser associado à política FPolicy. • Um mecanismo externo contém informações exigidas pelo nó para enviar notificações para um servidor FPolicy. • Você pode configurar o FPolicy para usar o mecanismo externo nativo do ONTAP para bloqueio de arquivos simples ou para usar um mecanismo externo configurado para usar servidores FPolicy externos (servidores FPolicy) para bloqueio de arquivos e gerenciamento de arquivos mais sofisticados. • Se você quiser usar o mecanismo externo nativo, você não pode especificar um valor para esse parâmetro ou pode especificar `native` como o valor. • Se você quiser usar servidores FPolicy, a configuração para o mecanismo externo já deve existir.	`-engine engine_name`	Sim (a menos que a política use o mecanismo nativo do ONTAP interno)	`native`

É obrigatório rastreio Especifica se a triagem obrigatória de acesso a arquivos é necessária. • A configuração de triagem obrigatória determina qual ação é tomada em um evento de acesso a arquivos em um caso em que todos os servidores primário e secundário estão inativos ou nenhuma resposta é recebida dos servidores FPolicy dentro de um determinado período de tempo limite. • Quando definido como `true`, os eventos de acesso ao arquivo são negados. • Quando definido como `false`, eventos de acesso a arquivos são permitidos.	`-is-mandatory {true`	`false`Selecione	Não

`true`	*Permitir acesso privilegiado* Especifica se você deseja que o servidor FPolicy tenha acesso privilegiado aos arquivos e pastas monitorados usando uma conexão de dados privilegiada. Se configurado, os servidores FPolicy podem acessar arquivos da raiz do SVM que contém os dados monitorados usando a conexão de dados privilegiada. Para acesso privilegiado a dados, o SMB deve ser licenciado no cluster e todas as LIFs de dados usadas para se conetar aos servidores FPolicy devem ser configuradas para ter `cifs` como um dos protocolos permitidos. Se você quiser configurar a diretiva para permitir acesso privilegiado, você também deve especificar o nome de usuário para a conta que deseja que o servidor FPolicy use para acesso privilegiado.	`-allow -privileged -access {yes`	`no`Selecione

Não (a menos que a leitura de passagem esteja ativada)	`no`	*Nome de usuário privilegiado* Especifica o nome de usuário da conta que os servidores FPolicy usam para acesso privilegiado a dados. • O valor para este parâmetro deve usar o formato "nome de usuário". • Se `-allow -privileged -access` estiver definido como `no`, qualquer valor definido para este parâmetro será ignorado.	`-privileged -user-name user_name`

Não (a menos que o acesso privilegiado esteja ativado)	Nenhum	*Permitir passagem-leitura* Especifica se os servidores FPolicy podem fornecer serviços de leitura de passagem para arquivos que foram arquivados em armazenamento secundário (arquivos off-line) pelos servidores FPolicy: • A passagem-leitura é uma maneira de ler dados para arquivos off-line sem restaurar os dados para o armazenamento primário. A passagem-leitura reduz as latências de resposta porque não há necessidade de recuperar arquivos de volta ao storage primário antes de responder à solicitação de leitura. Além disso, a passagem-leitura otimiza a eficiência de storage eliminando a necessidade de consumir espaço de storage primário com arquivos que são recuperados exclusivamente para atender às solicitações de leitura. Quando ativado,	`-is-passthrough -read-enabled {true`

Requisito para configurações de escopo FPolicy se a política FPolicy usar o mecanismo nativo

Se você configurar a política FPolicy para usar o mecanismo nativo, há um requisito específico para como definir o escopo FPolicy configurado para a política.

O escopo FPolicy define os limites nos quais a política FPolicy se aplica, por exemplo, se a FPolicy se aplica a volumes ou compartilhamentos especificados. Existem vários parâmetros que restringem ainda mais o escopo ao qual a política FPolicy se aplica. Um desses parâmetros, `-is-file-extension-check-on-directories-enabled`, especifica se deve verificar as extensões de arquivo nos diretórios. O valor padrão é `false`, o que significa que as extensões de arquivo nos diretórios não estão marcadas.

Quando uma diretiva FPolicy que usa o mecanismo nativo está ativada em um compartilhamento ou volume e o `-is-file-extension-check-on-directories-enabled` parâmetro é definido como `false` para o escopo da política, o acesso ao diretório é negado. Com essa configuração, como as extensões de arquivo não são verificadas para diretórios, qualquer operação de diretório é negada se ela estiver sob o escopo da política.

Para garantir que o acesso ao diretório seja bem-sucedido ao usar o mecanismo nativo, você deve definir o `-is-file-extension-check-on-directories-enabled` parâmetro para `true` ao criar o escopo.

Com este parâmetro definido como `true`, as verificações de extensão acontecem para operações de diretório e a decisão de permitir ou negar acesso é tomada com base nas extensões incluídas ou excluídas na configuração do escopo FPolicy.

Preencha a Planilha de política FPolicy

Você pode usar essa Planilha para Registrar os valores necessários durante o processo de configuração da política FPolicy. Você deve Registrar se deseja incluir cada configuração de parâmetro na configuração da política FPolicy e, em seguida, Registrar o valor para os parâmetros que deseja incluir.

Tipo de informação	Incluir	Seus valores
Nome da máquina virtual de storage (SVM)	Sim	
Nome da política	Sim	
Nomes de eventos	Sim	
Armazenamento persistente		
Nome do motor externo		
É necessário um rastreio obrigatório?		
Permitir acesso privilegiado		
Nome de usuário privilegiado		

A leitura de passagem está ativada?		

Planeje a configuração do escopo do FPolicy

Planeje a visão geral da configuração do escopo da FPolicy

Antes de configurar o escopo FPolicy, você deve entender o que significa criar um escopo. Você deve entender o que a configuração do escopo contém. Você também precisa entender quais são as regras de escopo de precedência. Essas informações podem ajudá-lo a Planejar os valores que você deseja definir.

O que significa criar um escopo FPolicy

Criar o escopo FPolicy significa definir os limites nos quais a política FPolicy se aplica. A máquina virtual de storage (SVM) é o limite básico. Ao criar um escopo para uma política de FPolicy, você deve definir a política de FPolicy à qual será aplicada e designar a qual SVM você deseja aplicar o escopo.

Há vários parâmetros que restringem ainda mais o escopo dentro do SVM especificado. Você pode restringir o escopo especificando o que incluir no escopo ou especificando o que excluir do escopo. Depois de aplicar um escopo a uma política habilitada, as verificações de eventos de política são aplicadas ao escopo definido por este comando.

As notificações são geradas para eventos de acesso a arquivos onde as correspondências são encontradas nas opções "'include'". As notificações não são geradas para eventos de acesso a arquivos em que as correspondências são encontradas nas opções "'excluir'".

A configuração do escopo da FPolicy define as seguintes informações de configuração:

- Nome do SVM
- Nome da política
- As ações a incluir ou excluir do que é monitorado
- As políticas de exportação para incluir ou excluir do que é monitorado
- Os volumes a incluir ou excluir do que é monitorado
- As extensões de arquivo para incluir ou excluir do que é monitorado
- Se a extensão de arquivo deve ser feita verifica em objetos de diretório

> Existem considerações especiais para o escopo de uma política de FPolicy de cluster. A política de FPolicy de cluster é uma política que o administrador do cluster cria para o SVM admin. Se o administrador do cluster também criar o escopo dessa política de FPolicy do cluster, o administrador SVM não poderá criar um escopo para essa mesma política. No entanto, se o administrador do cluster não criar um escopo para a política de FPolicy do cluster, qualquer administrador SVM poderá criar o escopo dessa política de cluster. Se o administrador do SVM criar um escopo para essa política de FPolicy de cluster, o administrador do cluster não poderá criar posteriormente um escopo de cluster para essa mesma política de cluster. Isso ocorre porque o administrador do cluster não pode substituir o escopo da mesma diretiva de cluster.

Quais são as regras de escopo de precedência

As seguintes regras de precedência se aplicam às configurações do escopo:

- Quando um compartilhamento é incluído no `-shares-to-include` parâmetro e o volume pai do compartilhamento é incluído no `-volumes-to-exclude` parâmetro, `-volumes-to-exclude` tem precedência sobre `-shares-to-include`.
- Quando uma política de exportação é incluída no `-export-policies-to-include` parâmetro e o volume pai da política de exportação é incluído no `-volumes-to-exclude` parâmetro, `-volumes-to-exclude` tem precedência sobre `-export-policies-to-include`.
- Um administrador pode especificar as `-file-extensions-to-include` listas e `-file-extensions-to-exclude` .

  O `-file-extensions-to-exclude` parâmetro é verificado antes de o `-file-extensions-to-include` parâmetro ser verificado.

O que contém a configuração do escopo do FPolicy

Você pode usar a seguinte lista de parâmetros de configuração do escopo FPolicy disponíveis para ajudá-lo a Planejar sua configuração:

> Ao configurar quais compartilhamentos, políticas de exportação, volumes e extensões de arquivo para incluir ou excluir do escopo, os parâmetros incluir e excluir podem incluir metacaracters como ""?" `and` "*". O uso de expressões regulares não é suportado.

Tipo de informação	Opção
SVM Especifica o nome do SVM no qual você deseja criar um escopo FPolicy. Cada configuração de FPolicy é definida em um único SVM. O mecanismo externo, o evento de política, o escopo da política e a política que se combinam para criar uma configuração de política FPolicy devem estar associados ao mesmo SVM.	`-vserver vserver_name`
Nome da política Especifica o nome da política FPolicy à qual você deseja anexar o escopo. A política FPolicy já deve existir.	`-policy-name policy_name`
Compartilhamentos para incluir Especifica uma lista delimitada por vírgulas de compartilhamentos para monitorar a política FPolicy à qual o escopo é aplicado.	`-shares-to-include share_name, ...`

Compartilhamentos para excluir Especifica uma lista delimitada por vírgulas de compartilhamentos a serem excluídos do monitoramento para a política FPolicy à qual o escopo é aplicado.	`-shares-to-exclude share_name, ...`
Volumes a incluir especifica uma lista delimitada por vírgulas de volumes a monitorar para a política FPolicy à qual o escopo é aplicado.	`-volumes-to-include volume_name, ...`
Volumes a excluir Especifica uma lista delimitada por vírgulas de volumes a excluir do monitoramento para a política FPolicy à qual o escopo é aplicado.	`-volumes-to-exclude volume_name, ...`
Exportar políticas para incluir Especifica uma lista delimitada por vírgulas de políticas de exportação para monitorar a política FPolicy à qual o escopo é aplicado.	`-export-policies-to -include export_policy_name, ...`
Exportar políticas para excluir Especifica uma lista delimitada por vírgulas de políticas de exportação para excluir do monitoramento da política FPolicy à qual o escopo é aplicado.	`-export-policies-to -exclude export_policy_name, ...`
Extensões de arquivo para incluir Especifica uma lista delimitada por vírgulas de extensões de arquivo para monitorar a política FPolicy à qual o escopo é aplicado.	`-file-extensions-to -include file_extensions, ...`
Extensão de arquivo para excluir Especifica uma lista delimitada por vírgulas de extensões de arquivo para excluir do monitoramento da política FPolicy à qual o escopo é aplicado.	`-file-extensions-to -exclude file_extensions, ...`
A verificação de extensão de arquivo no diretório está ativada ? Especifica se as verificações de extensão de nome de arquivo também se aplicam a objetos de diretório. Se esse parâmetro estiver definido como `true`, os objetos de diretório serão submetidos às mesmas verificações de extensão que os arquivos normais. Se esse parâmetro estiver definido como `false`, os nomes dos diretórios não serão correlacionados para extensões e as notificações serão enviadas para diretórios, mesmo que suas extensões de nome não correspondam. Se a política FPolicy ao qual o escopo é atribuído estiver configurada para usar o mecanismo nativo, esse parâmetro deverá ser definido como `true`.	`-is-file-extension -check-on-directories -enabled{true false`

Preencha a folha de cálculo do escopo da FPolicy

Você pode usar essa Planilha para Registrar os valores necessários durante o processo de configuração do escopo do FPolicy. Se um valor de parâmetro for necessário, você precisará determinar qual valor usar para esses parâmetros antes de configurar o escopo FPolicy.

Você deve Registrar se deseja incluir cada configuração de parâmetro na configuração do escopo do FPolicy e, em seguida, Registrar o valor dos parâmetros que deseja incluir.

Tipo de informação	Obrigatório	Incluir	Seus valores
Nome da máquina virtual de storage (SVM)	Sim	Sim	
Nome da política	Sim	Sim	
Compartilhamentos a incluir	Não		
Compartilhamentos a excluir	Não		
Volumes a incluir	Não		
Volumes a excluir	Não		
Políticas de exportação a incluir	Não		
Exportar políticas para excluir	Não		
Extensões de arquivo a incluir	Não		
Extensão do ficheiro a excluir	Não		
A verificação de extensão de arquivo no diretório está ativada?	Não		

Informações sobre direitos autorais

Informações sobre marcas comerciais