



Crie a configuração FPolicy

ONTAP 9

NetApp
January 17, 2025

Índice

- Crie a configuração FPolicy 1
 - Crie o mecanismo externo FPolicy 1
 - Crie o evento FPolicy 2
 - Criar armazenamentos persistentes FPolicy 3
 - Crie a política FPolicy 5
 - Crie o escopo FPolicy 7
 - Ative a política FPolicy 8

Crie a configuração FPolicy

Crie o mecanismo externo FPolicy

Você deve criar um mecanismo externo para começar a criar uma configuração FPolicy. O mecanismo externo define como o FPolicy faz e gerencia conexões com servidores FPolicy externos. Se sua configuração usar o mecanismo interno do ONTAP (o mecanismo externo nativo) para bloqueio de arquivos simples, você não precisará configurar um mecanismo externo FPolicy separado e não precisará executar esta etapa.

O que você vai precisar

A "[motor externo](#)" folha de trabalho deve ser concluída.

Sobre esta tarefa

Se o mecanismo externo for usado em uma configuração do MetroCluster, você deverá especificar os endereços IP dos servidores FPolicy no site de origem como servidores primários. Os endereços IP dos servidores FPolicy no local de destino devem ser especificados como servidores secundários.

Passos

1. Crie o mecanismo externo FPolicy usando o `vserver fpolicy policy external-engine create` comando.

O comando a seguir cria um mecanismo externo na máquina virtual de storage (SVM) `vs1.example.com`. Não é necessária autenticação para comunicações externas com o servidor FPolicy.

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

2. Verifique a configuração do mecanismo externo FPolicy usando o `vserver fpolicy policy external-engine show` comando.

O comando a seguir exibe informações sobre todos os mecanismos externos configurados no SVM `vs1.example.com`:

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

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

O comando a seguir exibe informações detalhadas sobre o mecanismo externo chamado "Engine1" no

SVM vs1.example.com:

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

```

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

Crie o evento FPolicy

Como parte da criação de uma configuração de política FPolicy, você precisa criar um evento FPolicy. Você associa o evento à política FPolicy quando ele é criado. Um evento define qual protocolo monitorar e quais eventos de acesso ao arquivo monitorar e filtrar.

Antes de começar

Você deve concluir o evento FPolicy "[folha de trabalho](#)".

Crie o evento FPolicy

1. Crie o evento FPolicy usando o `vserver fpolicy policy event create` comando.

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

2. Verifique a configuração do evento FPolicy usando o `vserver fpolicy policy event show` comando.

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

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

Crie os eventos Acesso negado FPolicy

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.

1. Crie o evento FPolicy usando o `vserver fpolicy policy event create` comando.

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

Criar armazenamentos persistentes FPolicy

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 9.14,1, 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.

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.

Há duas maneiras de criar um armazenamento persistente, dependendo da versão do ONTAP:

- ONTAP 9.15,1 ou posterior: Quando você cria o armazenamento persistente, o ONTAP cria e configura automaticamente seu volume ao mesmo tempo. Isso simplifica a configuração de armazenamento persistente do FPolicy e implementa todas as práticas recomendadas.
- ONTAP 9.14,1: Crie e configure manualmente um volume e, em seguida, crie um armazenamento persistente para o volume recém-criado.

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.

Criar um armazenamento persistente (ONTAP 9.15,1 ou posterior)

A partir do ONTAP 9.15,1, use o `fpolicy persistent-store create` comando para criar o armazenamento persistente FPolicy com criação e configuração de volume inline. O ONTAP bloqueia automaticamente o volume do acesso ao protocolo de usuário externo (CIFS/NFS).

Antes de começar

- O SVM em que você deseja criar o armazenamento persistente deve ter pelo menos um agregado.
- Você deve ter acesso aos agregados disponíveis para o SVM e permissões suficientes para criar volumes.

Passos

1. Crie o armazenamento persistente, que cria e configura o volume automaticamente:

```
vserver fpolicy persistent-store create -vserver <vserver> -persistent-store
```

```
<name> -volume <volume_name> -size <size> -autosize-mode  
<off|grow|grow_shrink>
```

- O `vserver` parâmetro é o nome do SVM.
- O `persistent-store` parâmetro é o nome do armazenamento persistente.
- O `volume` parâmetro é o nome do volume de armazenamento persistente.



Se você quiser usar um volume vazio existente, use o `volume show` comando para localizá-lo e especificá-lo no parâmetro `volume`.

- O `size` parâmetro é baseado na duração do tempo para o qual você deseja persistir os eventos que não são entregues ao servidor externo (aplicativo parceiro).

Por exemplo, se você quiser que 30 minutos de eventos persistam em um cluster com uma capacidade de 30K notificações por segundo:

Tamanho de volume necessário: 30000 x 30 x 60 x 0,6KB (tamanho médio do Registro de notificação): 32400000 KB, aproximadamente 32 GB

Para encontrar a taxa de notificação aproximada, você pode entrar em Contato com seu aplicativo de parceiro FPolicy ou utilizar o contador FPolicy `requests_dispatched_rate`.



Se você estiver usando um volume existente, o parâmetro tamanho é opcional. Se você fornecer um valor para o parâmetro tamanho, ele modificará o volume com o tamanho especificado.

- O `autosize-mode` parâmetro especifica o modo de dimensionamento automático para o volume. Os modos de dimensionamento automático suportados são:
 - Desligado - o volume não cresce nem diminui em tamanho em resposta à quantidade de espaço usado.
 - Crescer - o volume cresce automaticamente quando o espaço usado no volume está acima do limite de crescimento.
 - `Grow_shrink` - o volume cresce ou encolhe em tamanho em resposta à quantidade de espaço usado.

2. Crie a política FPolicy e adicione o nome do armazenamento persistente a essa política. Para obter mais informações, "[Crie a política FPolicy](#)" consulte .

Criar um armazenamento persistente (ONTAP 9.14,1)

Você pode criar um volume e, em seguida, criar um armazenamento persistente para usar esse volume. Em seguida, você pode bloquear o volume recém-criado do acesso de protocolo de usuário externo (CIFS/NFS).

Passos

1. Crie um volume vazio na SVM que possa ser provisionado para o armazenamento persistente:

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

Espera-se que um usuário administrador com Privileges RBAC suficiente (para criar um volume) crie um

volume (usando o comando da cli de volume ou API REST) do tamanho desejado e forneça o nome desse volume como o `-volume` comando criar CLI no armazenamento persistente ou API REST.

- O `vserver` parâmetro é o nome do SVM.
- O `volume` parâmetro é o nome do volume de armazenamento persistente.
- O `state` parâmetro deve ser definido como `online` para que o volume esteja disponível para uso.
- O `policy` parâmetro é definido para a política de serviço FPolicy, se você já tiver um configurado. Caso contrário, você pode usar o `volume modify` comando mais tarde para adicionar a política.
- O `unix-permissions` parâmetro é opcional.
- O `size` parâmetro é baseado na duração do tempo para o qual você deseja persistir os eventos que não são entregues ao servidor externo (aplicativo parceiro).

Por exemplo, se você quiser que 30 minutos de eventos persistam em um cluster com uma capacidade de 30K notificações por segundo:

Tamanho de volume necessário: $30000 \times 30 \times 60 \times 0,6\text{KB}$ (tamanho médio do Registro de notificação): 32400000 KB, aproximadamente 32 GB

Para encontrar a taxa de notificação aproximada, você pode entrar em Contato com seu aplicativo de parceiro FPolicy ou utilizar o contador `FPolicy requests_dispatched_rate`.

- O parâmetro agregado é necessário para volumes FlexVol, caso contrário não é necessário.
- O `snapshot-policy` parâmetro deve ser definido como `nenhum`. Isso garante que não haja restauração acidental do snapshot levando à perda de eventos atuais e impede o possível processamento de eventos duplicados.

Se você quiser usar um volume vazio existente, use o `volume show` comando para encontrá-lo e o `volume modify` comando para fazer as alterações necessárias. Certifique-se de que a política, o tamanho e `snapshot-policy` os parâmetros estão definidos corretamente para o armazenamento persistente.

2. Crie o armazenamento persistente:

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

- O `vserver` parâmetro é o nome do SVM.
- O `persistent-store` parâmetro é o nome do armazenamento persistente.
- O `volume` parâmetro é o nome do volume de armazenamento persistente.

3. Crie a política FPolicy e adicione o nome do armazenamento persistente a essa política. Para obter mais informações, "[Crie a política FPolicy](#)" consulte .

Crie a política FPolicy

Ao criar a política FPolicy, você associa um mecanismo externo e um ou mais eventos à política. A política também especifica se a triagem obrigatória é necessária, se os servidores FPolicy têm acesso privilegiado aos dados na máquina virtual de

armazenamento (SVM) e se a leitura de passagem para arquivos off-line está ativada.

O que você vai precisar

- A Planilha de política FPolicy deve ser concluída.
- Se você planeja configurar a política para usar servidores FPolicy, o mecanismo externo deve existir.
- Deve existir pelo menos um evento FPolicy que pretende associar à política FPolicy.
- Se você quiser configurar o acesso a dados privilegiados, um servidor SMB deve existir na SVM.
- Para configurar um armazenamento persistente para uma política, o tipo de mecanismo deve ser **assíncrono** e a política deve ser **não obrigatória**.

Para obter mais informações, "[Crie armazenamentos persistentes](#)" consulte .

Passos

1. Crie a política FPolicy:

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

- Você pode adicionar um ou mais eventos à política FPolicy.
- Por predefinição, a seleção obrigatória está ativada.
- Se você quiser permitir acesso privilegiado definindo o `-allow-privileged-access` parâmetro como `yes`, você também deve configurar um nome de usuário privilegiado para acesso privilegiado.
- Se você quiser configurar a passagem-leitura definindo o `-is-passthrough-read-enabled` parâmetro como `true`, você também deve configurar o acesso privilegiado a dados.

O comando a seguir cria uma política chamada "policy1" que tem o evento chamado ""event1"" e o motor externo chamado ""Engine1"" associado a ele. Esta política usa valores padrão na configuração da política: `vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

O comando a seguir cria uma política chamada "policy2" que tem o evento chamado ""event2"" e o motor externo chamado ""engine2"" associado a ele. Esta política é configurada para usar o acesso privilegiado usando o nome de usuário especificado. A passagem-leitura está ativada:

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

O comando a seguir cria uma política chamada "native1" que tem o evento chamado ""event3"" associado a ele. Esta política usa o mecanismo nativo e usa valores padrão na configuração da política:

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

2. Verifique a configuração da diretiva FPolicy usando o `vserver fpolicy policy show` comando.

O comando a seguir exibe informações sobre as três políticas FPolicy configuradas, incluindo as seguintes informações:

- O SVM associado à política
- O motor externo associado à política
- Os eventos associados à política
- Se é necessária uma triagem obrigatória
- Se o acesso privilegiado é necessário `vserver fpolicy policy show`

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

Crie o escopo FPolicy

Depois de criar a política FPolicy, você precisa criar um escopo FPolicy. Ao criar o escopo, você associa o escopo a uma política FPolicy. Um escopo define os limites nos quais a política FPolicy se aplica. Os escopos podem incluir ou excluir arquivos com base em compartilhamentos, políticas de exportação, volumes e extensões de arquivo.

O que você vai precisar

A folha de trabalho do âmbito da FPolicy tem de ser concluída. A política FPolicy deve existir com um mecanismo externo associado (se a política estiver configurada para usar servidores FPolicy externos) e deve ter pelo menos um evento FPolicy associado.

Passos

1. Crie o escopo FPolicy usando o `vserver fpolicy policy scope create` comando.

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

2. Verifique a configuração do escopo do FPolicy usando o `vserver fpolicy policy scope show` comando.

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

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

Ative a política FPolicy

Depois de configurar uma configuração de política FPolicy, você ativa a política FPolicy. A ativação da política define sua prioridade e inicia o monitoramento de acesso a arquivos para a política.

O que você vai precisar

A política FPolicy deve existir com um mecanismo externo associado (se a política estiver configurada para usar servidores FPolicy externos) e deve ter pelo menos um evento FPolicy associado. O escopo da política FPolicy deve existir e deve ser atribuído à política FPolicy.

Sobre esta tarefa

A prioridade é usada quando várias políticas são habilitadas na máquina virtual de storage (SVM) e mais de uma política é subscrita ao mesmo evento de acesso a arquivos. As políticas que usam a configuração nativa do mecanismo têm uma prioridade maior do que as políticas para qualquer outro mecanismo, independentemente do número de sequência atribuído a elas ao ativar a política.



Não é possível ativar uma política no SVM do administrador.

Passos

1. Ative a política FPolicy usando o `vserver fpolicy enable` comando.

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

2. Verifique se a política FPolicy está ativada usando o `vserver fpolicy show` comando.

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

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

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.