



Planeie a configuração da política FPolicy

ONTAP 9

NetApp
January 17, 2025

Índice

- Planeie a configuração da política FPolicy 1
 - Planeje a visão geral da configuração da política FPolicy 1
 - Requisito para configurações de escopo FPolicy se a política FPolicy usar o mecanismo nativo 7
 - Preencha a Planilha de política FPolicy 7

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
<i>Nome da SVM</i> Especifica o nome do SVM no qual você deseja criar uma política de FPolicy.	<code>-vserver</code> <code>vserver_name</code>	Sim	Nenhum

<p><i>Nome da política</i></p> <p>Especifica o nome da política FPolicy.</p> <p>O nome pode ter até 256 caracteres.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p>O nome deve ter até 200 caracteres se a diretiva estiver configurada em uma configuração de recuperação de desastres do MetroCluster ou SVM.</p> </div> <p>O nome pode conter qualquer combinação dos seguintes caracteres de intervalo ASCII:</p> <ul style="list-style-type: none"> • a através z • A através Z • 0 através 9 • "»_", "-", and "»." 	<p>-policy-name policy_name</p>	<p>Sim</p>	<p>Nenhum</p>
<p><i>Nomes de eventos</i></p> <p>Especifica uma lista delimitada por vírgulas de eventos a serem associados à política FPolicy.</p> <ul style="list-style-type: none"> • 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. 	<p>-events event_name, ...</p>	<p>Sim</p>	<p>Nenhum</p>
<p><i>Armazenamento persistente</i></p> <p>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.</p>	<p>-persistent -store persistent_store_name</p>	<p>Não</p>	<p>Nenhum</p>

<p><i>Nome externo do motor</i></p> <p>Especifica o nome do mecanismo externo a ser associado à política FPolicy.</p> <ul style="list-style-type: none"> • 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 <code>native</code> como o valor. • Se você quiser usar servidores FPolicy, a configuração para o mecanismo externo já deve existir. 	<pre>-engine engine_name</pre>	<p>Sim (a menos que a política use o mecanismo nativo do ONTAP interno)</p>	<p><code>native</code></p>
<p><i>É obrigatório rastreamento</i></p> <p>Especifica se a triagem obrigatória de acesso a arquivos é necessária.</p> <ul style="list-style-type: none"> • 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 <code>true</code>, os eventos de acesso ao arquivo são negados. • Quando definido como <code>false</code>, eventos de acesso a arquivos são permitidos. 	<pre>-is-mandatory {true</pre>	<p><code>false`</code> Selecione</p>	<p>Não</p>

true	<p><i>Permitir acesso privilegiado</i></p> <p>Especifica se você deseja que o servidor FPolicy tenha acesso privilegiado aos arquivos e pastas monitorados usando uma conexão de dados privilegiada.</p> <p>Se configurado, os servidores FPolicy podem acessar arquivos da raiz do SVM que contém os dados monitorados usando a conexão de dados privilegiada.</p> <p>Para acesso privilegiado a dados, o SMB deve ser licenciado no cluster e todas as LIFs de dados usadas para se conectar aos servidores FPolicy devem ser configuradas para ter <code>cifs</code> como um dos protocolos permitidos.</p> <p>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.</p>	<p>-allow -privileged -access {yes</p>	`no`Selecione
------	---	--	---------------

<p>Não (a menos que a leitura de passagem esteja ativada)</p>	<p>no</p>	<p><i>Nome de usuário privilegiado</i></p> <p>Especifica o nome de usuário da conta que os servidores FPolicy usam para acesso privilegiado a dados.</p> <ul style="list-style-type: none"> • O valor para este parâmetro deve usar o formato "nome de usuário". • Se <code>-allow -privileged -access</code> estiver definido como <code>no</code>, qualquer valor definido para este parâmetro será ignorado. 	<p><code>-privileged</code> <code>-user-name</code> <code>user_name</code></p>
---	-----------	---	--

<p>Não (a menos que o acesso privilegiado esteja ativado)</p>	<p>Nenhum</p>	<p><i>Permitir passagem-leitura</i></p> <p>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:</p> <ul style="list-style-type: none"> • A passagem-leitura é uma maneira de ler dados para arquivos off-line sem restaurar os dados para o armazenamento primário. <p>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.</p>	<pre>-is-passthrough -read-enabled {true</pre>
---	---------------	--	--

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

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, as extensões de arquivo não são verificadas para diretórios, qualquer operação de diretório é negada e a diretiva não permite acesso a diretórios. Se você quiser configurar a política para permitir acesso a diretórios, defina o `-is-file-extension-check-on-directories-enabled` parâmetro como `true` para 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` parameter 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 rastreo obrigatório?		
Permitir acesso privilegiado		

Nome de usuário privilegiado		
A leitura de passagem está ativada?		

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.