



Pianificare la configurazione del criterio FPolicy

ONTAP 9

NetApp
April 24, 2024

Sommario

- Pianificare la configurazione del criterio FPolicy 1
 - Pianificare la panoramica della configurazione dei criteri FPolicy 1
 - Requisito per le configurazioni dell'ambito FPolicy se il criterio FPolicy utilizza il motore nativo 7
 - Completare il foglio di lavoro della policy FPolicy 7

Pianificare la configurazione del criterio FPolicy

Pianificare la panoramica della configurazione dei criteri FPolicy

Prima di configurare il criterio FPolicy, è necessario comprendere quali parametri sono necessari per la creazione del criterio e perché si desidera configurare determinati parametri opzionali. Queste informazioni consentono di determinare i valori da impostare per ciascun parametro.

Quando si crea un criterio FPolicy, si associa il criterio a quanto segue:

- La macchina virtuale per lo storage (SVM)
- Uno o più eventi FPolicy
- Un motore esterno FPolicy

È inoltre possibile configurare diverse impostazioni opzionali dei criteri.

Contenuto della configurazione del criterio FPolicy

Per pianificare la configurazione, è possibile utilizzare il seguente elenco di criteri FPolicy obbligatori e parametri opzionali:

Tipo di informazione	Opzione	Obbligatorio	Predefinito
Nome SVM Specifica il nome della SVM su cui si desidera creare un criterio FPolicy.	<code>-vserver</code> <code>vserver_name</code>	Sì	Nessuno

<p><i>Nome policy</i></p> <p>Specifica il nome del criterio FPolicy.</p> <p>Il nome può contenere fino a 256 caratteri.</p> <div data-bbox="167 386 220 441"> </div> <p>Se si configura il criterio in una configurazione di disaster recovery MetroCluster o SVM, il nome deve contenere fino a 200 caratteri.</p> <p>Il nome può contenere qualsiasi combinazione dei seguenti caratteri ASCII:</p> <ul style="list-style-type: none"> • a attraverso z • A attraverso Z • 0 attraverso 9 • “_”, “-”, and “`” 	<p>-policy-name policy_name</p>	<p>Sì</p>	<p>Nessuno</p>
<p><i>Nomi eventi</i></p> <p>Specifica un elenco delimitato da virgole di eventi da associare al criterio FPolicy.</p> <ul style="list-style-type: none"> • È possibile associare più di un evento a un criterio. • Un evento è specifico di un protocollo. • È possibile utilizzare un singolo criterio per monitorare gli eventi di accesso ai file per più protocolli creando un evento per ciascun protocollo che si desidera monitorare dal criterio e associando quindi gli eventi al criterio. • Gli eventi devono già esistere. 	<p>-events event_name, ...</p>	<p>Sì</p>	<p>Nessuno</p>

<p>Nome motore esterno</p> <p>Specifica il nome del motore esterno da associare al criterio FPolicy.</p> <ul style="list-style-type: none"> • Un motore esterno contiene le informazioni richieste dal nodo per inviare le notifiche a un server FPolicy. • È possibile configurare FPolicy per utilizzare il motore esterno nativo di ONTAP per un semplice blocco dei file o per utilizzare un motore esterno configurato per utilizzare server FPolicy esterni (server FPolicy) per un blocco dei file e una gestione dei file più sofisticati. • Se si desidera utilizzare il motore esterno nativo, non è possibile specificare un valore per questo parametro o è possibile specificare <code>native</code> come valore. • Se si desidera utilizzare i server FPolicy, la configurazione per il motore esterno deve già esistere. 	<p><code>-engine</code> <code>engine_name</code></p>	<p>Sì (a meno che il criterio non utilizzi il motore nativo ONTAP interno)</p>	<p><code>native</code></p>
<p>È richiesto lo screening obbligatorio</p> <p>Specifica se è richiesto lo screening obbligatorio dell'accesso ai file.</p> <ul style="list-style-type: none"> • L'impostazione di screening obbligatorio determina l'azione intrapresa in caso di evento di accesso al file in caso di inattività di tutti i server primari e secondari o di mancata ricezione di una risposta dai server FPolicy entro un determinato periodo di timeout. • Quando è impostato su <code>true</code>, gli eventi di accesso al file sono negati. • Quando è impostato su <code>false</code>, sono consentiti eventi di accesso al file. 	<p><code>-is-mandatory</code> <code>{true</code></p>	<p><code>false}</code></p>	<p>No</p>

true	<p>Consenti accesso privilegiato</p> <p>Specifica se si desidera che il server FPolicy disponga di un accesso privilegiato ai file e alle cartelle monitorati utilizzando una connessione dati con privilegi.</p> <p>Se configurati, i server FPolicy possono accedere ai file dalla directory principale della SVM contenente i dati monitorati utilizzando la connessione dati con privilegi.</p> <p>Per un accesso privilegiato ai dati, SMB deve essere concesso in licenza sul cluster e tutti i dati LIF utilizzati per connettersi ai server FPolicy devono essere configurati in modo da avere <code>cifs</code> come uno dei protocolli consentiti.</p> <p>Se si desidera configurare il criterio per consentire l'accesso con privilegi, è necessario specificare anche il nome utente dell'account che il server FPolicy deve utilizzare per l'accesso con privilegi.</p>	<p>-allow -privileged -access {yes</p>	no}
------	---	--	-----

<p>No (a meno che non sia attivata la funzione pass-through-Read)</p>	<p>no</p>	<p><i>Nome utente privilegiato</i></p> <p>Specifica il nome utente dell'account utilizzato dai server FPolicy per l'accesso ai dati con privilegi.</p> <ul style="list-style-type: none"> • Il valore di questo parametro deve utilizzare il formato "<code>`domain` user name</code>". • Se <code>-allow-privileged</code> <code>-access</code> è impostato su <code>no</code>, qualsiasi valore impostato per questo parametro viene ignorato. 	<p><code>-privileged</code> <code>-user-name</code> <code>user_name</code></p>
---	-----------	--	--

<p>No (a meno che non sia abilitato l'accesso privilegiato)</p>	<p>Nessuno</p>	<p><i>Allow pass-through-Read</i></p> <p>Specifica se i server FPolicy possono fornire servizi di lettura pass-through per i file che sono stati archiviati nello storage secondario (file offline) dai server FPolicy:</p> <ul style="list-style-type: none"> • La lettura pass-through è un modo per leggere i dati per i file offline senza ripristinarli nello storage primario. <p>La funzione Passthrough-Read riduce le latenze delle risposte, poiché non è necessario richiamare i file sullo storage primario prima di rispondere alla richiesta di lettura. Inoltre, la funzione pass-through-Read ottimizza l'efficienza dello storage eliminando la necessità di consumare spazio di storage primario con file richiamati esclusivamente per soddisfare le richieste di lettura.</p> <ul style="list-style-type: none"> • Se attivati, i server FPolicy forniscono i dati per il file su un canale dati privilegiato 	<pre>-is-passthrough -read-enabled {true</pre>
---	----------------	---	--

Requisito per le configurazioni dell'ambito FPolicy se il criterio FPolicy utilizza il motore nativo

Se si configura il criterio FPolicy per utilizzare il motore nativo, esiste un requisito specifico per la definizione dell'ambito FPolicy configurato per il criterio.

L'ambito FPolicy definisce i limiti ai quali si applica il criterio FPolicy, ad esempio se FPolicy si applica a volumi o condivisioni specificati. Esistono diversi parametri che limitano ulteriormente l'ambito a cui si applica la policy FPolicy. Uno di questi parametri, `-is-file-extension-check-on-directories-enabled`, specifica se controllare le estensioni dei file nelle directory. Il valore predefinito è `false`, che significa che le estensioni dei file nelle directory non sono selezionate.

Quando un criterio FPolicy che utilizza il motore nativo è attivato su una condivisione o volume e su `-is-file-extension-check-on-directories-enabled` il parametro è impostato su `false` per l'ambito del criterio, l'accesso alla directory viene negato. Con questa configurazione, poiché le estensioni dei file non vengono controllate per le directory, qualsiasi operazione di directory viene negata se rientra nell'ambito del criterio.

Per garantire che l'accesso alla directory abbia esito positivo quando si utilizza il motore nativo, è necessario impostare `-is-file-extension-check-on-directories-enabled` parameter a `true` quando si crea l'ambito.

Con questo parametro impostato su `true`, i controlli delle estensioni vengono eseguiti per le operazioni di directory e la decisione di consentire o negare l'accesso viene presa in base alle estensioni incluse o escluse nella configurazione dell'ambito FPolicy.

Completare il foglio di lavoro della policy FPolicy

È possibile utilizzare questo foglio di lavoro per registrare i valori necessari durante il processo di configurazione dei criteri FPolicy. Registrare se si desidera includere ciascuna impostazione di parametro nella configurazione del criterio FPolicy e quindi registrare il valore dei parametri che si desidera includere.

Tipo di informazione	Includi	I tuoi valori
Nome SVM (Storage Virtual Machine)	Sì	
Nome policy	Sì	
Nomi degli eventi	Sì	
Nome del motore esterno		
È richiesto lo screening obbligatorio?		
Consentire l'accesso con privilegi		
Nome utente con privilegi		

Il pass-through-Read è abilitato?		
-----------------------------------	--	--

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.