



# Planen Sie die FPolicy-Konfiguration

ONTAP 9

NetApp  
March 22, 2023

# Inhaltsverzeichnis

- Planen Sie die FPolicy-Konfiguration ..... 1
  - Planen Sie die FPolicy-Konfiguration im Überblick ..... 1
  - Anforderung für FPolicy-Konfigurationen, wenn die FPolicy die native Engine verwendet ..... 7
  - Füllen Sie das FPolicy-Arbeitsblatt aus ..... 7

# Planen Sie die FPolicy-Konfiguration

## Planen Sie die FPolicy-Konfiguration im Überblick

Bevor Sie die FPolicy konfigurieren, müssen Sie verstehen, welche Parameter beim Erstellen der Richtlinie erforderlich sind sowie warum Sie bestimmte optionale Parameter konfigurieren möchten. Anhand dieser Informationen können Sie festlegen, welche Werte für jeden Parameter festgelegt werden sollen.

Beim Erstellen einer FPolicy verknüpfen Sie die Richtlinie mit der folgenden:


- Die Storage Virtual Machine (SVM)
- Ein oder mehrere FPolicy Events
- Eine externe FPolicy Engine

Sie können auch mehrere optionale Richtlinieneinstellungen konfigurieren.

### Was die FPolicy-Konfiguration enthält

Sie können die folgende Liste der erforderlichen FPolicy und optionalen Parameter verwenden, um Ihre Konfiguration zu planen:

Informationstyp	Option	Erforderlich	Standard
<i>SVM Name</i> Gibt den Namen der SVM an, auf der eine FPolicy erstellt werden soll.	<code>-vserver</code> <code>vserver_name</code>	Ja.	Keine

<p><i>Name der Richtlinie</i></p> <p>Gibt den Namen der FPolicy an.</p> <p>Der Name kann bis zu 256 Zeichen lang sein.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p>Wenn die Richtlinie in einer MetroCluster- oder SVM-Disaster-Recovery-Konfiguration konfiguriert ist, sollte der Name bis zu 200 Zeichen lang sein.</p> </div> <p>Der Name kann eine beliebige Kombination der folgenden Zeichen des ASCII-Bereichs enthalten:</p> <ul style="list-style-type: none"> <li>• a Bis z</li> <li>• A Bis Z</li> <li>• 0 Bis 9</li> <li>• „_“, „-“, and „.“</li> </ul>	<p>-policy-name policy_name</p>	<p>Ja.</p>	<p>Keine</p>
<p><i>Ereignisnamen</i></p> <p>Gibt eine kommagetrennte Liste von Ereignissen an, die mit der FPolicy verknüpft werden sollen.</p> <ul style="list-style-type: none"> <li>• Sie können einer Richtlinie mehrere Ereignisse zuordnen.</li> <li>• Ein Ereignis ist spezifisch für ein Protokoll.</li> <li>• Sie können eine einzelne Richtlinie verwenden, um Dateizugriffseignisse für mehr als ein Protokoll zu überwachen, indem Sie für jedes Protokoll, das die Richtlinie überwachen soll, ein Ereignis erstellen und dann die Ereignisse mit der Richtlinie verknüpfen.</li> <li>• Die Ereignisse müssen bereits vorhanden sein.</li> </ul>	<p>-events event_name, ...</p>	<p>Ja.</p>	<p>Keine</p>

<p><i>Name der externen Engine</i></p> <p>Gibt den Namen der externen Engine an, die mit der FPolicy verknüpft werden soll.</p> <ul style="list-style-type: none"> <li>• Eine externe Engine enthält die vom Knoten benötigten Informationen zum Senden von Benachrichtigungen an einen FPolicy-Server.</li> <li>• Sie können FPolicy so konfigurieren, dass die native externe ONTAP Engine zum einfachen Blockieren von Dateien oder zur Verwendung einer externen Engine verwendet wird, die für die Verwendung von externen FPolicy-Servern (FPolicy-Servern) konfiguriert ist, um anspruchsvollere Datei-Blockierung und Dateimanagement zu ermöglichen.</li> <li>• Wenn Sie die native externe Engine verwenden möchten, können Sie entweder keinen Wert für diesen Parameter angeben oder angeben <code>native</code> Als Wert.</li> <li>• Wenn Sie FPolicy-Server verwenden möchten, muss die Konfiguration für die externe Engine bereits vorhanden sein.</li> </ul>	<pre>-engine engine_name</pre>	<p>Ja (es sei denn, diese Richtlinie nutzt die interne ONTAP-native Engine)</p>	<p><code>native</code></p>
<p><i>Ist obligatorisches Screening erforderlich</i></p> <p>Gibt an, ob eine obligatorische Überprüfung des Dateizugriffs erforderlich ist.</p> <ul style="list-style-type: none"> <li>• Die obligatorische Screening-Einstellung legt fest, welche Maßnahmen bei einem Dateizugriff getroffen werden sollen, wenn alle primären und sekundären Server ausgefallen sind oder keine Antwort von den FPolicy-Servern innerhalb eines bestimmten Zeitlimits erhalten wird.</li> <li>• Wenn eingestellt auf <code>true</code>, Dateizugriffsereignisse werden verweigert.</li> <li>• Wenn eingestellt auf <code>false</code>, Dateizugriffsereignisse sind erlaubt.</li> </ul>	<pre>-is-mandatory {true</pre>	<pre>false}</pre>	<p>Nein</p>

<p>true</p>	<p><i>Privilegierten Zugriff zulassen</i></p> <p>Gibt an, ob der FPolicy-Server über eine privilegierte Datenverbindung privilegierten Zugriff auf die überwachten Dateien und Ordner haben soll.</p> <p>Bei entsprechender Konfiguration können FPolicy Server über die privilegierte Datenverbindung auf Dateien vom Root der SVM zugreifen, die die überwachten Daten enthalten.</p> <p>Für den privilegierten Datenzugriff muss SMB auf dem Cluster lizenziert sein. Alle Daten-LIFs für die Verbindung mit den FPolicy Servern müssen konfiguriert werden <code>cifs</code> Als eines der zulässigen Protokolle.</p> <p>Wenn Sie die Richtlinie so konfigurieren möchten, dass ein privilegierter Zugriff möglich ist, müssen Sie auch den Benutzernamen für das Konto angeben, das der FPolicy-Server für privilegierten Zugriff verwenden soll.</p>	<pre>-allow -privileged -access {yes</pre>	<pre>no}</pre>
-------------	--	--	----------------

<p>Nein (es sei denn, Passthrough-read ist aktiviert)</p>	<p>no</p>	<p><i>Privilegierter Benutzername</i></p> <p>Gibt den Benutzernamen des Kontos an, das FPolicy-Server für privilegierten Datenzugriff verwenden.</p> <ul style="list-style-type: none"> <li>• Der Wert für diesen Parameter sollte das Format „domain\user Name“ verwenden.</li> <li>• Wenn -allow -privileged -access ist auf festgelegt no, Jeder für diesen Parameter eingestellte Wert wird ignoriert.</li> </ul>	<p>-privileged -user-name user_name</p>
---	-----------	---	---

<p>Nein (sofern der privilegierte Zugriff nicht aktiviert ist)</p>	<p>Keine</p>	<p><i>Passthrough-read</i> zulassen</p> <p>Gibt an, ob die FPolicy-Server PassThrough-Read-Services für Dateien bereitstellen können, die von den FPolicy-Servern in sekundären Speicher (Offline-Dateien) archiviert wurden:</p> <ul style="list-style-type: none"> <li>• Passthrough-read ist eine Möglichkeit, Daten von Offline-Dateien zu lesen, ohne die Daten auf den primären Speicher wiederherzustellen.</li> </ul> <p>Durch das Passthrough-Lesevorgang werden die Reaktionszeiten reduziert, da vor der Reaktion auf die Leseanforderung keine Dateien zurück auf den primären Storage zurückgerufen werden müssen. Zusätzlich optimiert das Passthrough-Lesevorgang die Storage-Effizienz, da es nicht mehr erforderlich ist, primären Storage mit Dateien zu belegen, die ausschließlich für Lesezugriffe abgerufen werden.</p>	<p>-is-passthrough -read-enabled {true</p>
--	--------------	---	--



# Anforderung für FPolicy-Konfigurationen, wenn die FPolicy die native Engine verwendet

Wenn Sie die FPolicy so konfigurieren, dass die native Engine verwendet wird, gibt es eine spezifische Anforderung dafür, wie Sie den FPolicy-Umfang definieren, der für die Richtlinie konfiguriert ist.

FPolicy-Umfang definiert die Grenzen, über die die FPolicy gilt, zum Beispiel, ob FPolicy auf bestimmte Volumes oder Freigaben angewendet wird. Es gibt eine Reihe von Parametern, die den Geltungsbereich der FPolicy weiter einschränken. Einer dieser Parameter, `-is-file-extension-check-on-directories-enabled`, Gibt an, ob Dateierweiterungen auf Verzeichnissen überprüft werden sollen. Der Standardwert ist `false`, Das bedeutet, dass Dateierweiterungen auf Verzeichnissen nicht überprüft werden.

Wenn eine FPolicy, die die native Engine nutzt, auf einem Share oder Volume aktiviert wird `-is-file-extension-check-on-directories-enabled` Parameter festgelegt `false` Für den Umfang der Richtlinie wird der Zugriff auf das Verzeichnis verweigert. `Die` Dateierweiterungen nicht auf Verzeichnisse überprüft werden, wird bei dieser Konfiguration ein Verzeichnisverzug verweigert, wenn er unter den Geltungsbereich der Richtlinie fällt.

Um sicherzustellen, dass der Verzeichniszugriff erfolgreich ist, wenn Sie die native Engine verwenden, müssen Sie den festlegen `-is-file-extension-check-on-directories-enabled` konfiguriert parameter `is true` Beim Erstellen des Anwendungsbereichs.

Wenn dieser Parameter auf gesetzt ist `true`, Erweiterungsprüfungen erfolgen für Verzeichnisvorgänge und die Entscheidung, ob der Zugriff erlaubt oder verweigert wird, wird auf Grundlage der in der FPolicy Scope-Konfiguration enthaltenen oder ausgeschlossenen Erweiterungen getroffen.

## Füllen Sie das FPolicy-Arbeitsblatt aus

Mit diesem Arbeitsblatt können Sie die Werte erfassen, die Sie während der Konfiguration der Richtlinien für FPolicy benötigen. Sie sollten aufzeichnen, ob Sie die einzelnen Parametereinstellungen in die FPolicy-Konfiguration aufnehmen möchten, und dann den Wert für die Parameter notieren, die Sie einbeziehen möchten.

Informationstyp	Einschließlich	Ihre Werte
Name der Storage Virtual Machine (SVM)	Ja.	
Name der Richtlinie	Ja.	
Ereignisnamen	Ja.	
Name der externen Engine		
Ist ein obligatorisches Screening erforderlich?		
Privilegierten Zugriff zulassen		

Privilegierter Benutzername		
Ist Passthrough-read aktiviert?		

## Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.