Planung der FPolicy Richtlinienkonfiguration

ONTAP 9

NetApp
September 23, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nas-audit/plan-fpolicy-policy-config-concept.html on September 23, 2026. Always check docs.netapp.com for the latest.

Inhalt

Planung der FPolicy Richtlinienkonfiguration . . . 1
Informationen zu den Richtlinienkonfigurationen von ONTAP FPolicy . . . 1
Was die FPolicy Richtlinienkonfiguration enthält . . . 1
ONTAP FPolicy Bereichskonfigurationsanforderungen für die nativ Engine . . . 7
ONTAP FPolicy Richtlinien-Arbeitsblätter . . . 7

Planung der FPolicy Richtlinienkonfiguration

Informationen zu den Richtlinienkonfigurationen von ONTAP FPolicy

Bevor Sie die FPolicy Richtlinie konfigurieren, ist es wichtig zu verstehen, welche Parameter beim Erstellen der Richtlinie erforderlich sind und aus welchen Gründen bestimmte optionale Parameter konfiguriert werden können. Diese Informationen unterstützen dabei, die passenden Werte für jeden Parameter festzulegen.

Beim Erstellen einer FPolicy Richtlinie wird die Richtlinie mit den folgenden Elementen verknüpft:

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

Sie können außerdem verschiedene optionale Richtlinieneinstellungen konfigurieren.

Was die FPolicy Richtlinienkonfiguration enthält

Die folgende Liste der verfügbaren erforderlichen und optionalen Parameter der FPolicy Richtlinie unterstützt bei der Planung Ihrer Konfiguration:

Art der Information	Option	Erforderlich	Standard
SVM Name Gibt den Namen der SVM an, auf der eine FPolicy Richtlinie erstellt werden soll.	`-vserver vserver_name`	Ja	Keine

Richtlinienname Gibt den Namen der FPolicy Richtlinie an. Der Name darf maximal 256 Zeichen lang sein. Der Name sollte bis zu 200 Zeichen lang sein, wenn die Richtlinie in einer MetroCluster oder SVM-Notfallwiederherstellungskonfiguration konfiguriert wird. Der Name kann jede beliebige Kombination der folgenden ASCII-Zeichen enthalten: • `a`durch `z` • `A`durch `Z` • `0`durch `9` • “_”, “-”, and “.”	`-policy-name policy_name`	Ja	Keine
Ereignisnamen Gibt eine durch Kommas getrennte Liste von Ereignissen an, die der FPolicy Richtlinie zugeordnet werden. • Sie können einer Richtlinie mehrere Ereignisse zuordnen. • Ein Ereignis ist spezifisch für ein Protokoll. • Sie können eine einzige Richtlinie verwenden, um Dateizugriffsereignisse für mehr als ein Protokoll zu überwachen, indem Sie für jedes Protokoll, das die Richtlinie überwachen soll, ein Ereignis erstellen und dann die Ereignisse der Richtlinie zuordnen. • Die Ereignisse müssen bereits existieren.	`-events event_name, ...`	Ja	Keine
Persistenter Speicher Ab ONTAP 9.14.1 gibt dieser Parameter den persistenten Speicher an, in dem Dateizugriffsereignisse für asynchron nicht obligatorische Richtlinien in der SVM erfasst werden.	`-persistent -store persistent_store_name`	Nein	Keine

Externer Engine Name Gibt den Namen der externen Engine an, die der FPolicy Richtlinie zugeordnet werden soll. • Eine externe Engine enthält Informationen, die der Knoten benötigt, um Benachrichtigungen an einen FPolicy Server zu senden. • Sie können FPolicy so konfigurieren, dass die ONTAP native externe Engine für einfache Dateiblockierung verwendet wird oder eine externe Engine genutzt wird, die für die Verwendung externer FPolicy Server (FPolicy Server) konfiguriert ist, um eine anspruchsvollere Dateiblockierung und Dateiverwaltung zu ermöglichen. • Wenn Sie die native externe Engine verwenden möchten, können Sie entweder keinen Wert für diesen Parameter angeben oder `native` als Wert angeben. • Wenn Sie FPolicy Server verwenden möchten, muss die Konfiguration für die externe Engine bereits vorhanden sein.	`-engine engine_name`	Ja (es sei denn, die Richtlinie verwendet die interne ONTAP native Engine)	`native`
Ist eine obligatorische Überprüfung erforderlich? Legt fest, ob eine obligatorische Dateizugriff-Überprüfung erforderlich ist. • Die Einstellung für die obligatorische Überprüfung legt fest, welche Maßnahmen bei einem Dateizugriff ergriffen werden, wenn alle primären und sekundären Server ausgefallen sind oder innerhalb eines bestimmten Zeitüberschreitungszeitraums keine Antwort von den FPolicy-Servern eingeht. • Wenn auf `true` gesetzt, werden Dateizugriffsereignisse verweigert. • Wenn auf `false` gesetzt, sind Dateizugriffsereignisse zulässig.	`-is-mandatory {true`	`false}`	Nein

`true`	*Privilegierten Zugriff erlauben* Legt fest, ob der FPolicy Server über eine privilegierte Datenverbindung privilegierten Zugriff auf die überwachten Dateien und Ordner erhält. Sofern konfiguriert, können FPolicy Server über die privilegierte Datenverbindung auf Dateien vom Stamm der SVM mit den überwachten Daten zugreifen. Für den privilegierten Datenzugriff muss SMB auf dem Cluster lizenziert sein und alle Daten-LIFs, die zur Verbindung mit den FPolicy-Servern verwendet werden, müssen so konfiguriert sein, dass `cifs` als eines der zulässigen Protokolle vorhanden ist. Wenn die Richtlinie so konfiguriert werden soll, dass privilegierter Zugriff zugelassen wird, muss auch der Benutzername für das Konto angegeben werden, das der FPolicy Server für privilegierten Zugriff verwendet.	`-allow -privileged -access {yes`	`no}`

Nein (es sei denn, passthrough-read ist aktiviert)	`no`	*Privilegierter Benutzername* Gibt den Benutzernamen des Kontos an, das die FPolicy Server für den privilegierten Datenzugriff verwenden. • Der Wert für diesen Parameter sollte das Format “Domäne\Benutzername” verwenden. • Wenn `-allow-privileged-access` auf `no` gesetzt ist, wird jeder für diesen Parameter festgelegte Wert ignoriert.	`-privileged-user-name user_name`

Nein (es sei denn, privilegierter Zugriff ist aktiviert)	Keine	*Passthrough-Read zulassen* Legt fest, ob die FPolicy Server Passthrough-Lesedienste für Dateien bereitstellen können, die von den FPolicy Servern auf einen Sekundärspeicher archiviert wurden (Offline-Dateien): • Passthrough-Read ist eine Methode, um Daten aus Offline-Dateien zu lesen, ohne die Daten auf den primären Speicher wiederherzustellen. Passthrough-read reduziert die Antwortzeiten, da Dateien nicht vor der Beantwortung einer Leseanfrage in den primären Speicher zurückgeholt werden müssen. Zudem optimiert Passthrough-read die Speichereffizienz, da kein primärer Speicherplatz mit Dateien belegt werden muss, die ausschließlich zum Erfüllen von Leseanfragen zurückgeholt	`-is-passthrough-read-enabled {true`

ONTAP FPolicy Bereichskonfigurationsanforderungen für die nativ Engine

Wenn die FPolicy-Richtlinie so konfiguriert wird, dass sie die native Engine verwendet, besteht eine spezifische Anforderung an die Definition des für die Richtlinie konfigurierten FPolicy-Bereichs.

Der FPolicy-Bereich definiert die Grenzen, innerhalb derer die FPolicy-Richtlinie gilt, beispielsweise ob die FPolicy für bestimmte Volumes oder Freigaben gilt. Es gibt eine Reihe von Parametern, die den Anwendungsbereich, auf den die FPolicy-Richtlinie angewendet wird, weiter einschränken. Einer dieser Parameter, `-is-file-extension-check-on-directories-enabled`, legt fest, ob Dateierweiterungen in Verzeichnissen geprüft werden. Der Standardwert ist `false`, was bedeutet, dass Dateierweiterungen in Verzeichnissen nicht geprüft werden.

Wenn eine FPolicy-Richtlinie, die die native Engine verwendet, für eine Freigabe oder ein Volume aktiviert ist und der `-is-file-extension-check-on-directories-enabled` Parameter auf `false` für den Geltungsbereich der Richtlinie gesetzt ist, wird der Verzeichniszugriff verweigert. Mit dieser Konfiguration, da die Dateierweiterungen für Verzeichnisse nicht geprüft werden, wird jede Verzeichnisoperation verweigert, die in den Geltungsbereich der Richtlinie fällt.

Um sicherzustellen, dass der Verzeichniszugriff bei Verwendung der nativen Engine erfolgreich ist, muss `-is -file-extension-check-on-directories-enabled parameter` auf `true` gesetzt werden, wenn der Bereich erstellt wird.

Wenn dieser Parameter auf `true` gesetzt ist, erfolgen Erweiterungsprüfungen bei Verzeichnisoperationen, und die Entscheidung, ob der Zugriff erlaubt oder verweigert wird, basiert auf den in der FPolicy Scope-Konfiguration ein- oder ausgeschlossenen Erweiterungen.

ONTAP FPolicy Richtlinien-Arbeitsblätter

Sie können dieses Arbeitsblatt verwenden, um die Werte zu erfassen, die Sie während des FPolicy Richtlinienkonfigurationsprozesses benötigen. Es sollte festgehalten werden, ob jede Parametereinstellung in die FPolicy Richtlinienkonfiguration einbezogen werden soll, und anschließend der Wert für die Parameter, die einbezogen werden sollen.

Art der Information	Enthalten	Ihre Werte
Name der Storage Virtual Machine (SVM)	Ja	
Richtlinienname	Ja	
Ereignisnamen	Ja	
Persistenter Speicher		
Name der externen Engine		
Ist eine obligatorische Überprüfung erforderlich?		
Privilegierter Zugriff		
Name des privilegierten Benutzers		
Ist Passthrough-Lesen aktiviert?		

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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 IRGENDEINER 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.