FPolicy für die Dateiüberwachung und -verwaltung auf SVMs verwenden

ONTAP 9

NetApp
November 05, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nas-audit/two-parts-fpolicy-solution-concept.html on November 05, 2026. Always check docs.netapp.com for the latest.

Inhalt

FPolicy für die Dateiüberwachung und -verwaltung auf SVMs verwenden . . . 1
FPolicy verstehen . . . 1
Informationen zu ONTAP FPolicy Lösungen . . . 1
ONTAP FPolicy synchron und asynchron Benachrichtigungen . . . 1
ONTAP FPolicy persistente Speicher . . . 2
ONTAP FPolicy Konfigurationstypen . . . 3
Rollen der Clusterkomponenten in der ONTAP FPolicy Implementierung . . . 4
Wie ONTAP FPolicy mit externen FPolicy Servern funktioniert . . . 4
Kommunikationsprozess zwischen Knoten und externem ONTAP FPolicy Server . . . 7
Informationen zu ONTAP FPolicy Diensten in SVM-Namensräumen . . . 8
Wie ONTAP FPolicy Passthrough-Read die Benutzerfreundlichkeit verbessert . . . 9
Die FPolicy Konfiguration planen . . . 10
Anforderungen und Best Practices für die ONTAP FPolicy Konfiguration . . . 10
ONTAP FPolicy Konfigurationen einrichten . . . 18
Die Konfiguration der externen FPolicy Engine planen . . . 19
Die FPolicy Ereigniskonfiguration planen . . . 29
Planung der FPolicy Richtlinienkonfiguration . . . 39
Planung der FPolicy Bereichskonfiguration . . . 46
Die FPolicy Konfiguration erstellen . . . 50
ONTAP FPolicy externe Engines erstellen . . . 50
ONTAP FPolicy-Ereignisse erstellen . . . 51
ONTAP FPolicy persistente Speicher erstellen . . . 52
ONTAP FPolicy-Richtlinien erstellen . . . 55
ONTAP FPolicy-Bereiche erstellen . . . 57
ONTAP FPolicy Richtlinien aktivieren . . . 58
FPolicy Konfigurationen verwalten . . . 58
FPolicy Konfigurationen anpassen . . . 58
Informationen zu FPolicy Konfigurationen . . . 59
FPolicy Serververbindungen verwalten . . . 62

FPolicy für die Dateiüberwachung und -verwaltung auf SVMs verwenden

FPolicy verstehen

Informationen zu ONTAP FPolicy Lösungen

FPolicy ist ein Dateizugriff Benachrichtigungs-Framework, das zur Überwachung und Verwaltung von Dateizugriffsereignissen auf Storage Virtual Machines (SVMs) mithilfe von Partnerlösungen verwendet wird. Partnerlösungen ermöglichen die Umsetzung verschiedener Anwendungsfälle wie Data Governance und Compliance, Ransomware-Schutz und Datenmobilität.

Zu den Partnerlösungen gehören sowohl von NetApp unterstützte Drittanbieterlösungen als auch die NetApp Produkte Workload Security und NetApp Data Classification.

Eine FPolicy Lösung besteht aus zwei Komponenten. Das ONTAP FPolicy Framework verwaltet Aktivitäten im Cluster und sendet Benachrichtigungen an Partner Application (auch External FPolicy Servers genannt). External FPolicy Servers verarbeiten die von ONTAP FPolicy gesendeten Benachrichtigungen, um die Anwendungsfälle der Kunden zu erfüllen.

Das ONTAP Framework erstellt und verwaltet die FPolicy Konfiguration, überwacht Dateiereignisse und sendet Benachrichtigungen an externe FPolicy Server. ONTAP FPolicy stellt die Infrastruktur bereit, die die Kommunikation zwischen externen FPolicy Servern und Storage Virtual Machine (SVM) Knoten ermöglicht.

Das FPolicy Framework verbindet sich mit externen FPolicy Servern und sendet Benachrichtigungen über bestimmte Dateisystemereignisse an die FPolicy Server, wenn diese Ereignisse durch Clientzugriffe ausgelöst werden. Die externen FPolicy Server verarbeiten die Benachrichtigungen und senden Antworten an den Knoten zurück. Was infolge der Benachrichtigungsverarbeitung geschieht, hängt von der Anwendung und davon ab, ob die Kommunikation zwischen dem Knoten und den externen Servern asynchron oder synchron ist.

ONTAP FPolicy synchron und asynchron Benachrichtigungen

FPolicy sendet Benachrichtigungen über die FPolicy Schnittstelle an externe FPolicy Server. Die Benachrichtigungen werden entweder im synchronen oder asynchronen Modus gesendet. Der Benachrichtigungsmodus bestimmt, was ONTAP nach dem Senden der Benachrichtigungen an die FPolicy Server tut.

- **Asynchrone Benachrichtigungen**

  Bei asynchronen Benachrichtigungen wartet der Knoten nicht auf eine Antwort vom FPolicy Server, was den Gesamtdurchsatz des Systems erhöht. Diese Art von Benachrichtigung ist für Anwendungen geeignet, bei denen der FPolicy Server nicht verlangt, dass aufgrund der Benachrichtigungsbewertung eine Aktion durchgeführt wird. Beispielsweise werden asynchrone Benachrichtigungen verwendet, wenn der Administrator einer Storage Virtual Machine (SVM) den Dateizugriff überwachen und Revisionsdateien protokollieren möchte.

  Wenn ein FPolicy-Server, der im asynchronen Modus arbeitet, einen Netzausfall erlebt, werden die während des Ausfalls generierten FPolicy-Benachrichtigungen auf dem Speicherknoten gespeichert. Wenn

der FPolicy-Server wieder online ist, wird er über die gespeicherten Benachrichtigungen informiert und kann diese vom Speicherknoten abrufen. Die Dauer, für die die Benachrichtigungen während eines Ausfalls gespeichert werden können, ist bis zu 10 Minuten konfigurierbar.

Ab ONTAP 9.14.1 ermöglicht FPolicy die Einrichtung eines persistenten Speichers zur Erfassung von Dateizugriffsereignissen für asynchrone, nicht obligatorische Richtlinien in der SVM. Persistente Speicher können die Client-E/A-Verarbeitung von der FPolicy-Benachrichtigungsverarbeitung entkoppeln, um die Client-Latenz zu reduzieren. Synchrone (obligatorische oder nicht obligatorische) und asynchron obligatorische Konfigurationen werden nicht unterstützt.

- **Synchrone Benachrichtigungen**

  Im synchronen Modus muss der FPolicy Server jede Benachrichtigung bestätigen, bevor der Clientvorgang fortgesetzt werden darf. Diese Art von Benachrichtigung wird verwendet, wenn eine Aktion aufgrund der Auswertung der Benachrichtigung erforderlich ist. Beispielsweise werden synchrone Benachrichtigungen verwendet, wenn der SVM Administrator Anfragen anhand von Kriterien, die auf dem externen FPolicy Server festgelegt sind, zulassen oder ablehnen möchte.

Synchrone und asynchrone Anwendungen

Es gibt viele Einsatzmöglichkeiten für FPolicy Anwendungen, sowohl asynchron als auch synchron.

Asynchrone Anwendungen sind solche, bei denen der externe FPolicy Server den Dateizugriff oder Verzeichniszugriff nicht verändert oder Daten auf der Storage Virtual Machine (SVM) modifiziert. Beispiel:

- Dateizugriff und Protokollierung
- Ressourcenmanagement

Synchrone Anwendungen sind solche, bei denen der Dateizugriff geändert oder Daten vom externen FPolicy Server modifiziert werden. Beispiel:

- Quotenmanagement
- Dateizugriffsblockierung
- Dateiarchivierung und hierarchische Speicherverwaltung
- Verschlüsselungs- und Entschlüsselungsdienste
- Komprimierungs- und Dekomprimierungsdienste

ONTAP FPolicy persistente Speicher

Persistente Speicher können die Client-E/A-Verarbeitung von der FPolicy-Benachrichtigungsverarbeitung entkoppeln, um die Client-Latenz zu reduzieren. Ab ONTAP 9.14.1 kann ein FPolicy persistenter Speicher eingerichtet werden, um Dateizugriffsereignisse für asynchron nicht obligatorische Richtlinien in der SVM zu erfassen. Synchrone (obligatorische oder nicht obligatorische) und asynchron obligatorische Konfigurationen werden nicht unterstützt.

Diese Funktion ist nur im externen Modus von FPolicy verfügbar. Die von Ihnen verwendete Partneranwendung muss diese Funktion unterstützen. Es empfiehlt sich, gemeinsam mit Ihrem Partner zu prüfen, ob diese FPolicy Konfiguration unterstützt wird.

Ab ONTAP 9.15.1 ist die Konfiguration des persistenten Speichers mit FPolicy vereinfacht. Der `persistent-`

`store create` Befehl automatisiert die Volume-Erstellung für die SVM und konfiguriert das Volume gemäß den Best Practices für persistente Speicher.

Weitere Informationen zu Best Practices für persistente Speicher sind unter "Anforderungen, Überlegungen und bewährte Verfahren für die Konfiguration von FPolicy" zu finden.

Informationen zum Hinzufügen persistenter Speicher sind unter "Persistente Speicher erstellen" zu finden.

ONTAP FPolicy Konfigurationstypen

Es gibt zwei grundlegende FPolicy Konfigurationstypen. Die eine Konfiguration verwendet externe FPolicy Server zur Verarbeitung und Bearbeitung von Benachrichtigungen. Die andere Konfiguration verwendet keine externen FPolicy Server, sondern nutzt stattdessen den internen, nativen FPolicy Server von ONTAP für die einfache Dateiblockierung anhand von Erweiterungen.

- **Externe FPolicy Serverkonfiguration**

  Die Benachrichtigung wird an den FPolicy-Server gesendet, der die Anfrage prüft und anhand von Regeln festlegt, ob der Knoten die angeforderte Dateioperation zulassen soll. Bei synchronen Richtlinien sendet der FPolicy-Server anschließend eine Antwort an den Knoten, um die angeforderte Dateioperation entweder zu erlauben oder zu blockieren.

- **Native FPolicy Serverkonfiguration**

  Die Benachrichtigung wird intern geprüft. Die Anfrage wird basierend auf den im FPolicy Bereich konfigurierten Dateierweiterungseinstellungen zugelassen oder abgelehnt.

  Hinweis: Abgelehnte Dateierweiterungsanfragen werden nicht protokolliert.

Wann eine native FPolicy Konfiguration erstellt werden sollte

Native FPolicy Konfigurationen nutzen die interne FPolicy Engine von ONTAP, um Dateivorgänge anhand der Dateierweiterung zu überwachen und zu blockieren. Diese Lösung erfordert keine externen FPolicy Server (FPolicy Server). Die Verwendung einer nativen Dateiblockierungskonfiguration ist dann angemessen, wenn diese einfache Lösung ausreicht.

Die native Dateiblockierung ermöglicht die Überwachung aller Dateivorgänge, die den konfigurierten Vorgangs- und Filterereignissen entsprechen, und anschließend wird der Zugriff auf Dateien mit bestimmten Erweiterungen verweigert. Dies ist die Standardkonfiguration.

Diese Konfiguration bietet eine Möglichkeit, den Dateizugriff ausschließlich anhand der Dateierweiterung zu blockieren. Beispielsweise kann zum Blockieren von Dateien mit `mp3` Erweiterungen eine Richtlinie so konfiguriert werden, dass Benachrichtigungen für bestimmte Vorgänge mit Ziel-Dateierweiterungen von `mp3` bereitgestellt werden. Die Richtlinie ist so konfiguriert, dass `mp3` Dateianfragen für Vorgänge, die Benachrichtigungen generieren, abgelehnt werden.

Folgendes gilt für native FPolicy Konfigurationen:

- Die gleichen Filter und Protokolle, die von der serverbasierten Dateiprüfung von FPolicy unterstützt werden, werden auch für native Dateiblockierung unterstützt.
- Native Dateiblockierungs- und FPolicy serverbasierte Dateifilteranwendungen können gleichzeitig konfiguriert werden.

Dazu können zwei separate FPolicy Richtlinien für die Storage Virtual Machine (SVM) konfiguriert werden, wobei eine für die native Dateiblockierung und eine für die FPolicy Server-basierte Dateiprüfung konfiguriert ist.

- Die native Dateiblockierungsfunktion filtert Dateien nur anhand ihrer Dateiendung und nicht anhand ihres Inhalts.
- Im Falle symbolischer Links verwendet die native Dateiblockierung die Dateierweiterung der Stammdatei.

Weitere Informationen zu "FPolicy: Native Dateiblockierung".

Wann eine Konfiguration erstellt wird, die externe FPolicy Server verwendet

FPolicy Konfigurationen, die externe FPolicy Server zur Verarbeitung und Verwaltung von Benachrichtigungen verwenden, bieten robuste Lösungen für Anwendungsfälle, in denen mehr als eine einfache Dateiblockierung auf Basis der Dateierweiterung erforderlich ist.

Eine Konfiguration, die externe FPolicy Server verwendet, ist sinnvoll, wenn beispielsweise Dateizugriffsereignisse überwacht und protokolliert werden sollen, Quotendienste bereitgestellt werden, Dateiblockierungen auf Grundlage anderer Kriterien als einfacher Dateierweiterungen erfolgen, Datenmigrationsdienste mithilfe hierarchischer Speicherverwaltungsanwendungen bereitgestellt werden oder ein fein abgestufter Satz von Richtlinien benötigt wird, der nur eine Teilmenge der Daten in der Storage Virtual Machine (SVM) überwacht.

Rollen der Clusterkomponenten in der ONTAP FPolicy Implementierung

Der Cluster, die darin enthaltenen Storage Virtual Machines (SVMs) und die Daten-LIFs spielen alle eine Rolle bei einer FPolicy Implementierung.

- **Cluster**

  Der Cluster enthält das FPolicy Management Framework und pflegt und verwaltet Informationen über alle FPolicy Konfigurationen im Cluster.

- **SVM**

  Eine FPolicy Konfiguration wird auf SVM-Ebene definiert. Der Geltungsbereich der Konfiguration ist die SVM, und sie wirkt sich ausschließlich auf SVM-Ressourcen aus. Eine SVM Konfiguration kann keine Dateizugriffsanfragen überwachen und Benachrichtigungen für Dateizugriffe versenden, die für Daten gestellt werden, die sich auf einer anderen SVM befinden.

  FPolicy Konfigurationen können auf der Admin-SVM definiert werden. Nachdem die Konfigurationen auf der Admin-SVM definiert wurden, sind sie in allen SVMs sichtbar und verwendbar.

- **Daten-LIFs**

  Die Verbindungen zu den FPolicy Servern werden über Daten-LIFs hergestellt, die zur SVM mit der FPolicy Konfiguration gehören. Die für diese Verbindungen verwendeten Daten-LIFs können auf die gleiche Weise übergeben werden wie Daten-LIFs, die für den normalen Clientzugriff verwendet werden.

Wie ONTAP FPolicy mit externen FPolicy Servern funktioniert

Nachdem FPolicy auf der Storage Virtual Machine (SVM) konfiguriert und aktiviert wurde, läuft FPolicy auf jedem Knoten, an dem die SVM beteiligt ist. FPolicy ist verantwortlich für

den Aufbau und die Aufrechterhaltung von Verbindungen zu externen FPolicy Servern (FPolicy Server), für die Verarbeitung von Benachrichtigungen sowie für die Verwaltung von Benachrichtigungen an und von FPolicy Servern.

Darüber hinaus hat FPolicy im Rahmen des Verbindungsmanagements folgende Verantwortlichkeiten:

- Stellt sicher, dass Dateibenachrichtigungen über die korrekte LIF an den FPolicy Server weitergeleitet werden.
- Gewährleistet, dass bei der Zuordnung mehrerer FPolicy Server zu einer Richtlinie ein Lastausgleich beim Senden von Benachrichtigungen an die FPolicy Server erfolgt.
- Versuche, die Verbindung wiederherzustellen, wenn die Verbindung zu einem FPolicy Server unterbrochen wird.
- Sendet die Benachrichtigungen über eine authentifizierte Sitzung an die FPolicy Server.
- Verwaltet die vom FPolicy Server eingerichtete Passthrough-Read-Datenverbindung zur Bearbeitung von Clientanfragen, wenn Passthrough-Read aktiviert ist.

Wie Kontrollkanäle für die FPolicy Kommunikation verwendet werden

FPolicy initiiert eine Steuerkanalverbindung zu einem externen FPolicy Server von den Daten-LIFs jedes Knotens einer Storage Virtual Machine (SVM). FPolicy verwendet Steuerkanäle zur Übertragung von Dateibenachrichtigungen, daher kann ein FPolicy Server je nach SVM-Topologie mehrere Steuerkanalverbindungen sehen.

Wie privilegierte Datenzugriffskanäle für synchronen Kommunikationsaustausch verwendet werden

Bei synchronen Anwendungsfällen greift der FPolicy Server über einen privilegierten Datenzugriffspfad auf Daten zu, die sich auf der Storage Virtual Machine (SVM) befinden. Der Zugriff über den privilegierten Pfad stellt dem FPolicy Server das gesamte Dateisystem zur Verfügung. Er kann auf Datendateien zugreifen, um Informationen zu sammeln, Dateien zu scannen, Dateien zu lesen oder in Dateien zu schreiben.

Da der externe FPolicy Server über den privilegierten Datenkanal auf das gesamte Dateisystem vom Stammverzeichnis der SVM aus zugreifen kann, muss die Verbindung über den privilegierten Datenkanal sicher sein.

Wie FPolicy Verbindungsinformationen mit privilegierten Datenzugriffskanälen verwendet werden

Der FPolicy Server stellt privilegierte Dateizugriffsverbindungen zu Cluster-Knoten her, indem er spezifische Windows-Benutzeranmeldeinformationen verwendet, die mit der FPolicy Konfiguration gespeichert sind. SMB ist das einzige unterstützte Protokoll für die Herstellung einer privilegierten Dateizugriffskanalverbindung.

Falls der FPolicy Server privilegierten Dateizugriff benötigt, müssen die folgenden Bedingungen erfüllt sein:

- Auf dem Cluster muss eine SMB-Lizenz aktiviert sein.
- Der FPolicy Server muss unter den in der FPolicy Konfiguration festgelegten Anmeldeinformationen ausgeführt werden.

Beim Herstellen einer Datenkanalverbindung verwendet FPolicy die Anmeldeinformationen für den angegebenen Windows-Benutzernamen. Der Dateizugriff erfolgt über die Adminfreigabe ONTAP_ADMIN$.

Was die Vergabe von Superuser-Berechtigungen für den Zugriff auf privilegierte Daten bedeutet

ONTAP verwendet die Kombination aus IP-Adresse und Benutzeranmeldeinformationen, die in der FPolicy Konfiguration festgelegt ist, um dem FPolicy Server Superuser-Berechtigungen zu erteilen.

Der Superuser-Status gewährt dem FPolicy Server die folgenden Berechtigungen beim Datenzugriff:

- Berechtigungsprüfungen vermeiden

  Der Benutzer umgeht Kontrollen des Datei- und Verzeichniszugriffs.

- Spezielle Sperrberechtigungen

  ONTAP ermöglicht Lese-, Schreib- oder Änderungszugriff auf beliebige Dateien, unabhängig von bestehenden Sperren. Wenn der FPolicy Server Bytebereichssperren für die Datei setzt, erfolgt die sofortige Entfernung bestehender Sperren für die Datei.

- Jegliche FPolicy-Prüfungen umgehen

  Access generiert keine FPolicy-Benachrichtigungen.

Wie FPolicy die Richtlinienverarbeitung verwaltet

Ihrer Storage Virtual Machine (SVM) können mehrere FPolicy Richtlinien mit jeweils unterschiedlicher Priorität zugewiesen sein. Für die Erstellung einer geeigneten FPolicy Konfiguration auf der SVM ist es wichtig zu verstehen, wie FPolicy die Richtlinienverarbeitung verwaltet.

Jede Dateizugriffsanfrage wird zunächst geprüft, um festzustellen, welche Richtlinien dieses Ereignis überwachen. Handelt es sich um ein überwachtes Ereignis, werden Informationen über das überwachte Ereignis sowie die relevanten Richtlinien an FPolicy übermittelt, wo sie ausgewertet werden. Jede Richtlinie wird in der Reihenfolge der zugewiesenen Priorität ausgewertet.

Folgende Empfehlungen sind bei der Konfiguration von Richtlinien zu berücksichtigen:

- Wenn eine Richtlinie immer vor anderen Richtlinien ausgewertet werden soll, wird diese Richtlinie mit einer höheren Priorität konfiguriert.
- Wenn der Erfolg einer angeforderten Dateizugriffsoperation bei einem überwachten Ereignis eine Voraussetzung für eine Dateianforderung ist, die anhand einer anderen Richtlinie ausgewertet wird, erhält die Richtlinie, die den Erfolg oder Misserfolg der ersten Dateioperation steuert, eine höhere Priorität.

  Wenn beispielsweise eine Richtlinie die Archivierungs- und Wiederherstellungsfunktionalität von FPolicy-Dateien verwaltet und eine zweite Richtlinie Dateizugriffsvorgänge auf die Online-Datei verwaltet, muss die Richtlinie, die die Dateiwiederherstellung verwaltet, eine höhere Priorität haben, damit die Datei wiederhergestellt wird, bevor der von der zweiten Richtlinie verwaltete Vorgang zugelassen werden kann.

- Wenn alle Richtlinien, die für einen Dateizugriff gelten könnten, ausgewertet werden sollen, ist synchronen Richtlinien eine niedrigere Priorität zuzuweisen.

Sie können die Prioritäten bestehender Richtlinien neu anordnen, indem Sie die Richtliniensequenznummer ändern. Damit FPolicy die Richtlinien jedoch anhand der geänderten Prioritätsreihenfolge auswertet, muss die Richtlinie mit der geänderten Sequenznummer deaktiviert und anschließend wieder aktiviert werden.

Kommunikationsprozess zwischen Knoten und externem ONTAP FPolicy Server

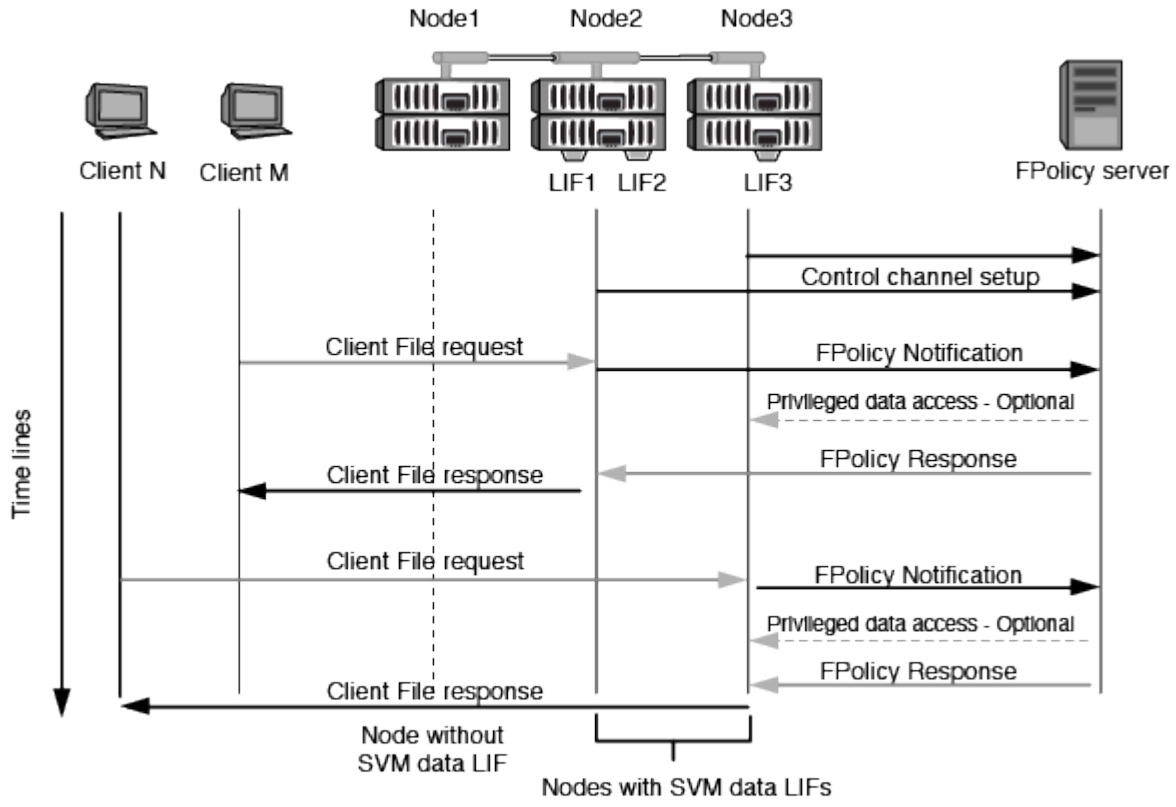
Für eine optimale Planung Ihrer FPolicy Konfiguration ist es wichtig, den Kommunikationsprozess zwischen dem Knoten und dem externen FPolicy Server zu verstehen.

Jeder Knoten, der an einer Storage Virtual Machine (SVM) beteiligt ist, initiiert eine Verbindung zu einem externen FPolicy Server (FPolicy Server) über TCP/IP. Verbindungen zu den FPolicy Servern werden über Knotendaten-LIFs eingerichtet, daher kann ein beteiligter Knoten nur dann eine Verbindung herstellen, wenn er über einen betriebsbereiten Daten-LIF für die SVM verfügt.

Jeder FPolicy-Prozess auf den teilnehmenden Knoten versucht, eine Verbindung zum FPolicy Server herzustellen, wenn die Richtlinie aktiviert ist. Dabei werden die in der Richtlinienkonfiguration angegebene IP-Adresse und der Port der FPolicy External Engine verwendet.

Die Verbindung stellt einen Steuerkanal von jedem an jedem SVM beteiligten Knoten zum FPolicy Server über die Daten-LIF her. Sind auf demselben beteiligten Knoten sowohl IPv4- als auch IPv6-Daten-LIF-Adressen vorhanden, versucht FPolicy, Verbindungen sowohl für IPv4 als auch für IPv6 herzustellen. Daher muss der FPolicy Server in einem Szenario, in dem sich das SVM über mehrere Knoten erstreckt oder sowohl IPv4- als auch IPv6-Adressen vorhanden sind, nach der Aktivierung der FPolicy Policy auf dem SVM auf mehrere Anfragen zum Aufbau von Steuerkanälen aus dem Cluster vorbereitet sein.

Besteht ein Cluster beispielsweise aus drei Knoten, Node1, Node2 und Node3, und sind die SVM-Daten-LIFs nur auf Node2 und Node3 verteilt, werden Kontrollkanäle unabhängig von der Verteilung der Daten-Volumes ausschließlich von Node2 und Node3 initiiert. Angenommen, Node2 verfügt über zwei Daten-LIFs, LIF1 und LIF2, die zur SVM gehören, und die initiale Verbindung erfolgt über LIF1. Fällt LIF1 aus, versucht FPolicy, einen Kontrollkanal über LIF2 herzustellen.



Wie FPolicy die externe Kommunikation während einer LIF-Migration oder eines Failovers verwaltet

Daten-LIFs können auf Datenports im selben Knoten oder auf Datenports auf einem entfernten Knoten migriert werden.

Wenn ein Daten-LIF ausfällt oder migriert wird, wird eine neue Steuerkanalverbindung zum FPolicy-Server hergestellt. FPolicy kann dann SMB- und NFS-Client-Anfragen, bei denen eine Zeitüberschreitung aufgetreten ist, erneut versuchen, sodass neue Benachrichtigungen an die externen FPolicy-Server gesendet werden. Der Node weist FPolicy-Serverantworten auf ursprüngliche, aufgrund von Zeitüberschreitung abgelaufene SMB- und NFS-Anfragen zurück.

Wie FPolicy die externe Kommunikation während eines Node-Failovers verwaltet

Wenn der Clusterknoten, der die für die FPolicy-Kommunikation verwendeten Datenports hostet, ausfällt, unterbricht ONTAP die Verbindung zwischen dem FPolicy-Server und dem Knoten.

Die Auswirkungen eines Cluster-Failovers auf den FPolicy Server lassen sich abmildern, indem die Failover-Policy so konfiguriert wird, dass der für die FPolicy-Kommunikation verwendete Datenport auf einen anderen aktiven Knoten migriert wird. Nach Abschluss der Migration wird eine neue Verbindung über den neuen Datenport hergestellt.

Wenn die Failover-Richtlinie nicht für die Migration des Datenports konfiguriert ist, muss der FPolicy Server warten, bis der ausgefallene Knoten wieder verfügbar ist. Nachdem der Knoten wieder verfügbar ist, wird von diesem Knoten aus eine neue Verbindung mit einer neuen Session ID initiiert.

> Der FPolicy Server erkennt Verbindungsabbrüche mithilfe der Keep-Alive-Protokollnachricht. Die Zeitüberschreitung für das Entfernen der Session ID wird bei der Konfiguration von FPolicy festgelegt. Die Standard-Zeitüberschreitung beträgt zwei Minuten.

Informationen zu ONTAP FPolicy Diensten in SVM-Namensräumen

ONTAP stellt einen einheitlichen Storage Virtual Machine (SVM) Namespace bereit. Volumes im gesamten Cluster werden durch Verbindungen zu einem einzigen logischen Dateisystem zusammengeführt. Der FPolicy Server ist mit der Namespace-Topologie vertraut und stellt FPolicy-Dienste im gesamten Namespace bereit.

Der Namensraum ist spezifisch für die SVM und innerhalb dieser enthalten, daher ist er nur im Kontext der SVM sichtbar. Namensräume weisen folgende Eigenschaften auf:

- In jedem SVM existiert ein einziger Namespace, dessen Wurzel das Root-Volume ist, das im Namespace als Schrägstrich (/) dargestellt wird.
- Alle anderen Volumen haben Verbindungspunkte unterhalb des Root-Verzeichnisses (/).
- Volumenverbindungen sind für Clients transparent.
- Ein einzelner NFS Export ermöglicht den Zugriff auf den gesamten Namensraum, alternativ können Exportrichtlinien bestimmte Volumes exportieren.
- SMB-Freigaben können auf dem Volume, auf Qtrees innerhalb des Volumes oder auf einem beliebigen Verzeichnis innerhalb des Namespace erstellt werden.
- Die Namensraumarchitektur ist flexibel.

  Beispiele für typische Namensraumarchitekturen sind wie folgt:

- Ein Namensraum mit einem einzigen Zweig vom Stammverzeichnis
- Ein Namensraum mit mehreren Zweigen vom Stammverzeichnis
- Ein Namespace mit mehreren unverzweigten Volumes vom Stammverzeichnis

Wie ONTAP FPolicy Passthrough-Read die Benutzerfreundlichkeit verbessert

Die Passthrough-read-Funktion ermöglicht dem FPolicy Server (der als hierarchischer Storage-Management-Server (HSM) fungiert), Lesezugriff auf Offline-Dateien zu bieten, ohne die Datei vom sekundären Storage-System auf das primäres Storage-System zurückholen zu müssen.

Wenn ein FPolicy-Server für die Bereitstellung von HSM für Dateien auf einem SMB-Server konfiguriert ist, erfolgt eine richtlinienbasierte Dateimigration, bei der die Dateien offline auf sekundärem Storage abgelegt werden und auf dem primären Storage-System lediglich eine Platzhalterdatei verbleibt. Obwohl diese Platzhalterdatei für Clients wie eine normale Datei erscheint, handelt es sich tatsächlich um eine Sparse-Datei mit der gleichen Größe wie die Originaldatei. Die Sparse-Datei hat das SMB-Offline-Bit gesetzt und verweist auf die tatsächliche Datei, die auf den sekundären Storage migriert wurde.

Üblicherweise muss, wenn eine Leseanfrage für eine Offline-Datei empfangen wird, der angeforderte Inhalt zurück in das primäre Storage-System geholt und anschließend über das primäre Storage-System abgerufen werden. Die Notwendigkeit, Daten zurück in das primäre Storage-System zu holen, hat mehrere unerwünschte Auswirkungen. Zu den unerwünschten Auswirkungen gehören die erhöhte Latenz bei Clientanfragen, die durch das Zurückholen des Inhalts vor der Beantwortung der Anfrage entsteht, sowie der erhöhte Speicherplatzbedarf für zurückgeholte Dateien auf dem primären Storage-System.

FPolicy passthrough-read ermöglicht es dem HSM-Server (dem FPolicy-Server), Lesezugriff auf migrierte, offline Dateien zu gewähren, ohne die Datei vom sekundären Storage-System auf das primäre Storage-System zurückholen zu müssen. Anstatt die Dateien auf das primäre Storage-System zurückzuholen, können Leseanfragen direkt vom sekundären Storage-System bedient werden.

Copy Offload (ODX) wird bei der FPolicy Passthrough-Read-Operation nicht unterstützt.

Passthrough-read verbessert die Benutzerfreundlichkeit durch folgende Vorteile:

- Leseanfragen können auch dann bearbeitet werden, wenn das primäre Storage-System nicht über genügend Speicherplatz verfügt, um die angeforderten Daten zurück in das primäre Storage-System zu übertragen.
- Besseres Kapazitäts- und Leistungsmanagement bei einem möglichen Anstieg des Datenabrufs, beispielsweise wenn ein Skript oder eine Backup-Lösung auf viele Offline-Dateien zugreifen muss.
- Leseanforderungen für Offline-Dateien in Snapshots können bedient werden.

  Da Snapshots schreibgeschützt sind, kann der FPolicy Server die Originaldatei nicht wiederherstellen, wenn sich die Stub-Datei in einem Snapshot befindet. Die Verwendung von passthrough-read eliminiert dieses Problem.

- Es können Richtlinien eingerichtet werden, die steuern, wann Leseanfragen durch Zugriff auf die Datei im sekundären Storage bedient werden und wann die Offline-Datei in das primäre Storage-System zurückgerufen werden soll.

  Auf dem HSM-Server kann beispielsweise eine Richtlinie erstellt werden, die festlegt, wie oft innerhalb eines bestimmten Zeitraums auf eine Offline-Datei zugegriffen werden darf, bevor diese zurück in das

primäre Storage-System migriert wird. Diese Art von Richtlinie vermeidet das erneute Abrufen von Dateien, auf die selten zugegriffen wird.

Wie Leseanfragen verwaltet werden, wenn FPolicy passthrough-read aktiviert ist

Es ist wichtig zu verstehen, wie Leseanforderungen verwaltet werden, wenn FPolicy passthrough-read aktiviert ist, damit die Konnektivität zwischen der Storage Virtual Machine (SVM) und den FPolicy Servern optimal konfiguriert werden kann.

Wenn FPolicy passthrough-read aktiviert ist und die SVM eine Anfrage für eine Offline-Datei empfängt, sendet FPolicy eine Benachrichtigung an den FPolicy-Server (HSM-Server) über den Standardverbindungskanal.

Nach Erhalt der Benachrichtigung liest der FPolicy Server die Daten aus dem in der Benachrichtigung angegebenen Dateipfad und sendet die angeforderten Daten über die zwischen dem SVM und dem FPolicy Server eingerichtete privilegierte Passthrough-Read-Datenverbindung an die SVM.

Nach dem Senden der Daten antwortet der FPolicy Server auf die Leseanfrage mit ALLOW oder DENY. Je nachdem, ob die Leseanfrage zugelassen oder abgelehnt wird, sendet ONTAP entweder die angeforderten Informationen oder eine Fehlermeldung an den Client.

Die FPolicy Konfiguration planen

Anforderungen und Best Practices für die ONTAP FPolicy Konfiguration

Bevor Sie FPolicy Konfigurationen auf Ihren Storage Virtual Machines (SVMs) erstellen und konfigurieren, sollten bestimmte Anforderungen, Überlegungen und Best Practices für die Konfiguration von FPolicy beachtet werden.

FPolicy Funktionen werden entweder über die Befehlszeile (CLI) oder über REST APIs konfiguriert.

Anforderungen für die Einrichtung von FPolicy

Bevor Sie FPolicy auf Ihrer Storage Virtual Machine (SVM) konfigurieren und aktivieren, müssen bestimmte Voraussetzungen beachtet werden.

- Alle Knoten im Cluster müssen eine Version von ONTAP ausführen, die FPolicy unterstützt.
- Wenn die ONTAP native FPolicy Engine nicht verwendet wird, müssen externe FPolicy Server (FPolicy Server) installiert sein.
- Die FPolicy Server müssen auf einem Server installiert sein, der von den Daten-LIFs der SVM erreichbar ist, auf der FPolicy Richtlinien aktiviert sind.

> Ab ONTAP 9.8 stellt ONTAP mit der Hinzufügung des `data-fpolicy-client` Service einen Client-LIF-Dienst für ausgehende FPolicy-Verbindungen bereit. "Weitere Informationen zu LIFs und Servicerichtlinien".

- Die IP-Adresse des FPolicy Servers muss in der externen Engine-Konfiguration der FPolicy Richtlinie als primärer oder sekundärer Server konfiguriert werden.
- Wenn die FPolicy Server über einen privilegierten Datenkanal auf Daten zugreifen, müssen die folgenden zusätzlichen Anforderungen erfüllt sein:
  - SMB muss auf dem Cluster lizenziert sein.

Der Zugriff auf privilegierte Daten erfolgt über SMB Verbindungen.

  - Für den Zugriff auf Dateien über den privilegierten Datenkanal muss ein Benutzeranmeldeinformation konfiguriert werden.
  - Der FPolicy Server muss unter den in der FPolicy Konfiguration festgelegten Anmeldeinformationen ausgeführt werden.
  - Alle Daten-LIFs, die zur Kommunikation mit den FPolicy-Servern verwendet werden, müssen so konfiguriert sein, dass `cifs` als eines der zulässigen Protokolle erlaubt ist.

    Dies umfasst auch die LIFs, die für Passthrough-Read-Verbindungen verwendet werden.

- Ab ONTAP 9.20.1 unterstützen FPolicy-Richtlinien S3-Ereignisse. Um FPolicy für S3-Objektereignisse zu konfigurieren, müssen die folgenden zusätzlichen Anforderungen erfüllt sein:
  - Alle Knoten im Cluster müssen ONTAP 9.20.1 oder höher ausführen. Cluster mit gemischten Versionen blockieren die S3 FPolicy Konfiguration, bis alle Knoten diese Funktion unterstützen.
  - Unterstützt werden nur NAS-Buckets, keine nativen S3-Buckets.
  - Ein externer FPolicy-Server, der das protobuf-Benachrichtigungsformat unterstützt. Das XML-Format wird für S3-Ereignisse nicht unterstützt.

Bewährte Verfahren und Empfehlungen zur Einrichtung von FPolicy

Bei der Einrichtung von FPolicy auf Storage Virtual Machines (SVMs) ist es ratsam, sich mit den allgemeinen Best Practices und Empfehlungen für die Konfiguration vertraut zu machen, damit die FPolicy Konfiguration eine robuste Überwachungsleistung und Ergebnisse bietet, die den Anforderungen entsprechen.

Spezifische Richtlinien zu Leistung, Dimensionierung und Konfiguration sind in der FPolicy-Partneranwendung zu beachten.

Persistente Speicher

Ab ONTAP 9.14.1 ermöglicht FPolicy die Einrichtung eines persistenten Speichers zur Erfassung von Dateizugriffsereignissen für asynchrone, nicht obligatorische Richtlinien in der SVM. Persistente Speicher können die Client-E/A-Verarbeitung von der FPolicy-Benachrichtigungsverarbeitung entkoppeln, um die Client-Latenz zu reduzieren. Synchrone (obligatorische oder nicht obligatorische) und asynchron obligatorische Konfigurationen werden nicht unterstützt.

- Vor der Verwendung der Funktionalität des persistenten Speichers ist sicherzustellen, dass Ihre Partneranwendungen diese Konfiguration unterstützen.
- Sie benötigen einen persistenten Speicher für jede SVM, bei der FPolicy aktiviert ist.
  - Auf jeder SVM kann nur ein persistenter Speicher eingerichtet werden. Dieser einzelne persistente Speicher muss für alle FPolicy Konfigurationen auf dieser SVM verwendet werden, selbst wenn die Richtlinien von verschiedenen Partnern stammen.
- ONTAP 9.15.1 oder höher:
  - Der persistente Speicher, sein Volume und seine Volume-Konfiguration werden beim Erstellen des persistenten Speichers automatisch verwaltet.
- ONTAP 9.14.1:
  - Der persistente Speicher, sein Volume und seine Volume-Konfiguration werden manuell verwaltet.
- Das persistente Speichervolume wird auf dem Knoten mit LIFs erstellt, bei denen erwartet wird, dass der maximale Datenverkehr von FPolicy überwacht wird.

    - ONTAP 9.15.1 oder höher: Volumes werden während der Erstellung des persistenten Speichers automatisch erstellt und konfiguriert.
    - ONTAP 9.14.1: Cluster-Administratoren müssen auf jeder SVM, auf der FPolicy aktiviert ist, ein Volume für den persistenten Speicher erstellen und konfigurieren.
- Wenn die im persistenten Speicher angesammelten Benachrichtigungen die Größe des bereitgestellten Volumens überschreiten, beginnt FPolicy, die eingehenden Benachrichtigungen mit entsprechenden EMS-Meldungen zu verwerfen.
    - ONTAP 9.15.1 oder höher: Zusätzlich zu dem `size` Parameter kann der `autosize-mode` Parameter dazu beitragen, dass das Volume in Abhängigkeit vom belegten Speicherplatz wächst oder schrumpft.
    - ONTAP 9.14.1: Der `size` Parameter wird bei der Volume-Erstellung konfiguriert, um ein maximales Limit festzulegen.
- Setzen Sie die Snapshot-Richtlinie für das persistente Speichervolume auf `none` statt auf `default`. Dies stellt sicher, dass kein versehentliches Wiederherstellen des Snapshots erfolgt, was zum Verlust aktueller Ereignisse führen könnte, und verhindert eine mögliche doppelte Ereignisverarbeitung.
    - ONTAP 9.15.1 oder höher: Der `snapshot-policy` Parameter wird bei der Erstellung des persistenten Speichers automatisch auf none gesetzt.
    - ONTAP 9.14.1: Der `snapshot-policy` Parameter wird `none` während der Volume-Erstellung konfiguriert.
- Das persistente Speichervolume sollte für den externen Benutzerprotokollzugriff (CIFS/NFS) unzugänglich gemacht werden, um eine versehentliche Beschädigung oder Löschung der persistent gespeicherten Ereignisdatensätze zu vermeiden.
    - ONTAP 9.15.1 oder höher: ONTAP blockiert das Volume während der Erstellung des persistenten Speichers automatisch für den Zugriff über externe Benutzerprotokolle (CIFS/NFS).
    - ONTAP 9.14.1: Nach der Aktivierung von FPolicy das Volume in ONTAP aushängen, um den Verbindungspfad zu entfernen. Dadurch ist der Zugriff über externe Benutzerprotokolle (CIFS/NFS) nicht mehr möglich.

Weitere Informationen finden Sie unter "FPolicy persistente Speicher" und "Persistente Speicher erstellen".

Failover und Rückgabe des persistenten Speichers

Der persistente Speicher bleibt im Zustand des letzten empfangenen Ereignisses, wenn ein unerwarteter Neustart erfolgt oder FPolicy deaktiviert und wieder aktiviert wird. Nach einer Übernahme werden neue Ereignisse vom Partnerknoten gespeichert und verarbeitet. Nach einer Rückgabe nimmt der persistente Speicher die Verarbeitung aller möglicherweise noch vorhandenen, nicht verarbeiteten Ereignisse wieder auf, die beim Node-Takeover entstanden sind. Live-Ereignisse erhalten Vorrang vor nicht verarbeiteten Ereignissen.

Wird das persistente Speichervolume innerhalb desselben SVM von einem Knoten auf einen anderen verschoben, werden auch die noch nicht verarbeiteten Benachrichtigungen auf den neuen Knoten übertragen. Sie müssen den `fpolicy persistent-store create` Befehl auf einem der beiden Knoten erneut ausführen, nachdem das Volume verschoben wurde, damit die ausstehenden Benachrichtigungen an den externen Server zugestellt werden.

Weitere Informationen zu `fpolicy persistent-store create` finden sich in der "ONTAP-Befehlsreferenz".

Richtlinienkonfiguration

Die Konfiguration der externen FPolicy Engine, der Ereignisse und des Gültigkeitsbereichs für SVMs kann die Gesamterfahrung und Sicherheit verbessern.

- Konfiguration der externen FPolicy Engine für SVMs:
  - Zusätzliche Sicherheitsmaßnahmen gehen mit Leistungseinbußen einher. Die Aktivierung der Secure Sockets Layer (SSL)-Kommunikation hat Auswirkungen auf die Leistung beim Zugriff auf Freigaben.
  - Die externe FPolicy Engine sollte mit mehr als einem FPolicy Server konfiguriert werden, um Ausfallsicherheit und hohe Verfügbarkeit der FPolicy Server-Benachrichtigungsverarbeitung zu gewährleisten.
- Konfiguration von FPolicy Ereignissen für SVMs:

  Die Überwachung von Dateivorgängen beeinflusst Ihre Gesamterfahrung. Beispielsweise verbessert das Filtern unerwünschter Dateivorgänge auf der Speicherseite Ihre Erfahrung. NetApp empfiehlt die folgende Konfiguration:

  - Überwachung der minimalen Arten von Dateivorgängen und Aktivierung der maximalen Anzahl von Filtern, ohne den Anwendungsfall zu beeinträchtigen.
  - Filter werden für getattr-, Lese-, Schreib-, Öffnungs- und Schließvorgänge verwendet. In SMB- und NFS-Home-Verzeichnisumgebungen ist der Anteil dieser Vorgänge hoch.
  - Nur erfolgreiche, vom S3-Client gesteuerte Operationen generieren Benachrichtigungen. Intern generierte Operationen (wie z. B. Objektablauf oder durch Snapshots ausgelöste Wiederherstellungen) generieren keine FPolicy-Benachrichtigungen.
  - Unterstützte S3-Operationen umfassen:
    - Objekterstellung (PUT, COPY und CompleteMultipartUpload)
    - Objektlöschung (DELETE und multi-delete)
    - Objekt-Tag (Tag PUT und Tag DELETE)

      GET- und Leseereignisse werden nicht überwacht.
  - Eine S3-Mehrfachlöschanforderung kann bis zu 1.000 Objekte löschen, FPolicy sendet jedoch für jedes erfolgreich gelöschte Objekt eine Benachrichtigung (der SHM-Slot ist auf 32 KB begrenzt). Die Kapazität des externen Servers ist entsprechend zu planen.
  - Mit dem FPolicy-Richtlinienbereich können Sie bestimmte NAS-Buckets anhand ihres Namens ein- oder ausschließen. Wenn ein konfigurierter Bucket-Name falsch geschrieben ist oder der Bucket gelöscht wurde, blockiert FPolicy keine Vorgänge, sondern generiert lediglich keine Benachrichtigungen für diesen Bucket.
- Konfiguration des FPolicy Bereichs für SVMs:

  Der Geltungsbereich der Richtlinien sollte auf die relevanten Speicherobjekte wie Freigaben, Volumes und Exporte beschränkt werden, anstatt sie für die gesamte SVM zu aktivieren. NetApp empfiehlt, die Verzeichniserweiterungen zu überprüfen. Wenn der `is-file-extension-check-on-directories-enabled` Parameter auf `true` gesetzt ist, werden Verzeichnisobjekte denselben Erweiterungsprüfungen unterzogen wie reguläre Dateien.

Einschränkungen von S3 FPolicy

Ab ONTAP 9.20.1 unterstützt FPolicy die Überwachung von S3-Objekten mit folgenden Einschränkungen:

- S3 FPolicy arbeitet ausschließlich im asynchronen, nicht obligatorischen Modus. Synchroner Modus, obligatorische Richtlinien und nativ Blockieren (Blockieren auf Basis von Dateierweiterungen) werden für S3-Ereignisse nicht unterstützt.
- Persistenter Speicher wird für S3 FPolicy-Benachrichtigungen nicht unterstützt.
- SSL/TLS wird für S3-Benachrichtigungen bei der Verbindung zur externen FPolicy Engine nicht unterstützt.
- Privilegierter Datenzugriff und Passthrough-Lesezugriff gelten nicht für S3 FPolicy.
- Eine garantierte Delivery wird nicht unterstützt. Benachrichtigungen erfolgen nur nach bestem Bemühen und können verloren gehen, wenn die Verbindung zum externen FPolicy-Server unterbrochen ist oder der Shared Memory Buffer (SHM) nach mehreren Wiederholungsversuchen voll bleibt.
- S3-Ereignisse unterstützen keine Benachrichtigungen über Zugriffsverweigerungen und fehlgeschlagene Vorgänge.

Netzwerkkonfiguration

Die Netzwerkverbindung zwischen dem FPolicy-Server und dem Controller sollte eine geringe Latenz aufweisen. NetApp empfiehlt, den FPolicy-Datenverkehr durch die Verwendung eines privaten Netzwerks vom Client-Datenverkehr zu trennen.

Darüber hinaus empfiehlt es sich, externe FPolicy Server (FPolicy Server) in unmittelbarer Nähe des Clusters mit einer hohen Bandbreite zu platzieren, um minimale Latenz und eine hohe Bandbreite zu gewährleisten.

> In einem Szenario, in dem der LIF für FPolicy-Datenverkehr auf einem anderen Port als der LIF für Client-Datenverkehr konfiguriert ist, kann der FPolicy-LIF aufgrund eines Portausfalls auf den anderen Knoten übergehen. Dadurch ist der FPolicy-Server von dem Knoten aus, der die FPolicy-Benachrichtigungen für Dateivorgänge generiert, nicht mehr erreichbar, sodass die FPolicy-Benachrichtigungen für Dateivorgänge auf diesem Knoten fehlschlagen. Um dieses Problem zu vermeiden, sollte sichergestellt sein, dass der FPolicy-Server über mindestens einen LIF auf dem Knoten erreichbar ist, um FPolicy-Anfragen für die auf diesem Knoten durchgeführten Dateivorgänge zu verarbeiten.

Hardwarekonfiguration

Der FPolicy Server kann entweder auf einem physischen Server oder auf einem virtuellen Server betrieben werden. Wenn sich der FPolicy Server in einer virtuellen Umgebung befindet, sollten dem virtuellen Server dedizierte Ressourcen (CPU, Netzwerk und Arbeitsspeicher) zugewiesen werden.

Das Verhältnis von Clusterknoten zu FPolicy Servern sollte optimiert werden, um eine Überlastung der FPolicy Server zu vermeiden, was zu Latenzen führen kann, wenn die SVM auf Clientanfragen reagiert. Das optimale Verhältnis hängt von der jeweiligen Partneranwendung ab, für die der FPolicy Server verwendet wird. NetApp empfiehlt, gemeinsam mit Partnern den geeigneten Wert zu bestimmen.

Konfiguration mit mehreren Richtlinien

Die FPolicy Richtlinie für natives Blockieren hat unabhängig von der Sequenznummer die höchste Priorität, und entscheidungsändernde Richtlinien haben eine höhere Priorität als andere. Die Priorität der Richtlinie hängt vom Anwendungsfall ab. NetApp empfiehlt die Zusammenarbeit mit Partnern, um die angemessene Priorität zu bestimmen.

Größenüberlegungen

FPolicy überwacht SMB- und NFS-Operationen direkt, sendet Benachrichtigungen an den externen Server und wartet auf eine Antwort, abhängig vom Kommunikationsmodus der externen Engine (synchron oder

asynchron). Dieser Prozess wirkt sich auf die Performance des SMB- und NFS-Zugriffs sowie auf die CPU-Ressourcen aus.

Um mögliche Probleme zu vermeiden, empfiehlt NetApp, gemeinsam mit Partnern die Umgebung zu bewerten und zu dimensionieren, bevor FPolicy aktiviert wird. Die Leistung wird durch verschiedene Faktoren beeinflusst, darunter die Anzahl der Benutzer, die Merkmale der Arbeitslast wie Operationen pro Benutzer und Datengröße, die Netzwerklatenz sowie Ausfälle oder Langsamkeit von Servern.

Leistung überwachen

FPolicy ist ein benachrichtigungsbasiertes System. Benachrichtigungen werden zur Verarbeitung an einen externen Server gesendet und eine Antwort wird an ONTAP zurückgesendet. Dieser Roundtrip-Prozess erhöht die Latenz für den Clientzugriff.

Die Überwachung der Leistungsindikatoren auf dem FPolicy Server und in ONTAP ermöglicht die Identifizierung von Engpässen in der Lösung und die Anpassung der Parameter für eine optimale Lösung. Beispielsweise hat eine erhöhte FPolicy Latenz eine kaskadierende Auswirkung auf die SMB- und NFS-Zugriffslatenz. Deshalb empfiehlt sich die Überwachung sowohl der Arbeitslast (SMB und NFS) als auch der FPolicy Latenz. Zusätzlich lassen sich in ONTAP Quality-of-Service-Richtlinien verwenden, um für jedes Volume oder jede SVM, die für FPolicy aktiviert ist, eine Arbeitslast festzulegen.

NetApp empfiehlt, den `statistics show –object workload` Befehl auszuführen, um Workload-Statistiken anzuzeigen. Zusätzlich sollten die folgenden Parameter überwacht werden:

- Durchschnittliche Latenzen für Lesen und Schreiben
- Gesamtzahl der Operationen
- Lese- und Schreibzähler

Die Leistung der FPolicy Subsysteme lässt sich mithilfe der folgenden FPolicy Zähler überwachen.

> Sie müssen sich im Diagnosemodus befinden, um Statistiken im Zusammenhang mit FPolicy zu erfassen.

Schritte

1. FPolicy-Zähler erfassen:
   a. `statistics start -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics start -object fpolicy_policy -instance <instance_name> -sample-id <ID>`
2. FPolicy-Zähler anzeigen:
   a. `statistics show -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics show -object fpolicy_server -instance <instance_name> -sample-id <ID>`

   Die `fpolicy`- und `fpolicy_server`-Zähler liefern Informationen zu verschiedenen Leistungsparametern, die in der folgenden Tabelle beschrieben sind.

Zähler	Beschreibung
fpolicy counters	abgebrochene Anfragen

Zähler	Beschreibung
Anzahl der Bildschirmanforderungen, für die die Verarbeitung auf der SVM abgebrochen wurde	Ereignisanzahl
Liste der Ereignisse, die eine Benachrichtigung auslösen	max_request_latency
Maximale Latenz bei Bildschirmanfragen	ausstehende_Anfragen
Gesamtzahl der laufenden Bildschirmanfragen	verarbeitete_Anfragen
Gesamtzahl der Bildschirmanforderungen, die auf dem SVM die fpolicy Verarbeitung durchlaufen haben	Anfragelatenz_hist
Histogramm der Latenz für Bildschirmanfragen	Anfragen-Auslieferungsrate
Anzahl der pro Sekunde versendeten Bildschirmanfragen	requests_received_rate
Anzahl der pro Sekunde empfangenen Bildschirmanfragen	**fpolicy_server-Zähler**
max_request_latency	Maximale Latenz für eine Bildschirmanfrage
ausstehende_Anfragen	Gesamtzahl der auf eine Antwort wartenden Bildschirmanfragen
Anfragelatenz	Durchschnittliche Latenz für Bildschirmanfrage
Anfragelatenz_hist	Histogramm der Latenz für Bildschirmanfragen
Anfrage-Sende-Rate	Anzahl der pro Sekunde an den FPolicy Server gesendeten Bildschirmanfragen
Antwortempfangsrate	Anzahl der vom FPolicy Server pro Sekunde empfangenen Bildschirmantworten

Weitere Informationen zu `statistics start` und `statistics show` finden sich in der "ONTAP-Befehlsreferenz".

FPolicy Workflow und Abhängigkeit von anderen Technologien verwalten

NetApp empfiehlt, eine FPolicy Richtlinie zu deaktivieren, bevor Konfigurationsänderungen vorgenommen werden. Wenn beispielsweise eine IP-Adresse in der für die aktivierte Richtlinie konfigurierten externen Engine hinzugefügt oder geändert werden soll, ist zuerst die Richtlinie zu deaktivieren.

Wenn FPolicy zur Überwachung von NetApp FlexCache Volumes konfiguriert wird, empfiehlt NetApp, FPolicy

nicht für die Überwachung von Lese- und getattr-Dateioperationen zu konfigurieren. Die Überwachung dieser Operationen in ONTAP erfordert den Abruf von Inode-zu-Pfad-Daten (I2P). Da I2P-Daten nicht von FlexCache Volumes abgerufen werden können, müssen sie vom Ursprungs-Volume abgerufen werden. Daher werden durch die Überwachung dieser Operationen die Performance Vorteile aufgehoben, die FlexCache bieten kann. Bei S3 NAS-Buckets auf FlexCache Volumes erzeugen interne Write-Back- und Write-Around-Operationen auf das Ursprungs-Volume keine FPolicy-Benachrichtigungen. Als Best Practice sollte FPolicy sowohl auf der Ursprungs-SVM als auch auf der FlexCache SVM konfiguriert werden, um alle S3-Ereignisse zu erfassen.

Wenn sowohl FPolicy als auch eine externe Antivirenlösung im Einsatz sind, erhält die Antivirenlösung die Benachrichtigungen zuerst. Die Verarbeitung durch FPolicy beginnt erst, nachdem der Antivirenscan abgeschlossen ist. Es ist wichtig, die Antivirenlösungen korrekt zu dimensionieren, da ein langsamer Antivirenscanner die Gesamtleistung beeinträchtigen kann.

S3 FPolicy wird für MetroCluster Konfigurationen unterstützt. Nach der Umschaltung können FPolicy-Benachrichtigungen vom entfernten (verbleibenden) Standort generiert werden, sofern der externe FPolicy-Server konfiguriert und von diesem Standort aus erreichbar ist.

Während der Übernahme und Rückgabe von Knoten kann die Verbindung zum FPolicy-Server kurzzeitig unterbrochen werden, wenn die zugehörige LIF auf einen anderen Knoten migriert. Die Verbindung wird automatisch wiederhergestellt, sobald eine geeignete LIF verfügbar ist. S3-Clients, die während dieses Zeitfensters Vorgänge erneut versuchen, generieren neue FPolicy-Benachrichtigungen, sobald die Verbindung wiederhergestellt ist.

Überlegungen zum Passthrough-Read-Upgrade und Revert

Es gibt bestimmte Aspekte beim Upgrade und Revertierung, die bekannt sein sollten, bevor auf eine ONTAP Version aktualisiert wird, die passthrough-read unterstützt, oder bevor auf eine Version zurückgekehrt wird, die passthrough-read nicht unterstützt.

Upgrade

Nachdem alle Knoten auf eine Version von ONTAP aktualisiert wurden, die FPolicy Passthrough-Read unterstützt, ist der Cluster in der Lage, die Passthrough-Read-Funktionalität zu nutzen; jedoch ist Passthrough-Read in bestehenden FPolicy Konfigurationen standardmäßig deaktiviert. Um Passthrough-Read in bestehenden FPolicy Konfigurationen zu verwenden, muss die FPolicy Richtlinie deaktiviert, die Konfiguration geändert und anschließend die Konfiguration wieder aktiviert werden.

Nachdem alle Knoten auf ONTAP 9.20.1 oder höher aktualisiert wurden, können FPolicy-Ereignisse mit dem S3-Protokoll und S3-Objektoperationen (object create, object delete, object tag) konfiguriert werden. In Clustern mit gemischten Versionen ist die S3 FPolicy Konfiguration gesperrt.

Wiederherstellung

Bevor auf eine Version von ONTAP zurückgekehrt wird, die FPolicy passthrough-read nicht unterstützt, müssen die folgenden Bedingungen erfüllt sein:

- Alle Richtlinien, die passthrough-read verwenden, deaktivieren und anschließend die betroffenen Konfigurationen so anpassen, dass sie passthrough-read nicht mehr verwenden.
- Die FPolicy Funktionalität im Cluster wird deaktiviert, indem jede FPolicy Richtlinie im Cluster deaktiviert wird.

Bevor auf eine Version von ONTAP zurückgekehrt wird, die keine persistenten Speicher unterstützt, muss sichergestellt sein, dass keine der FPolicy Richtlinien einen persistenten Speicher konfiguriert hat. Wenn ein persistenter Speicher konfiguriert ist, schlägt das Zurücksetzen fehl.

Vor der Rückkehr zu einer Version von ONTAP, die S3 FPolicy nicht unterstützt, müssen alle mit dem S3-Protokoll konfigurierten FPolicy-Ereignisse gelöscht werden. Wenn die S3 FPolicy Konfiguration bestehen bleibt, schlägt die Rückkehr fehl.

Verwandte Informationen

- "Statistiken zeigen"
- "Statistiken Start"

ONTAP FPolicy Konfigurationen einrichten

Bevor FPolicy den Dateizugriff überwachen kann, muss eine FPolicy Konfiguration auf der Storage Virtual Machine (SVM), für die FPolicy Dienste benötigt werden, erstellt und aktiviert werden.

Die Schritte zum Einrichten und Aktivieren einer FPolicy Konfiguration auf der SVM sind wie folgt:

1. Eine externe FPolicy Engine wird erstellt.

   Die externe FPolicy Engine identifiziert die externen FPolicy Server (FPolicy Server), die einer bestimmten FPolicy Konfiguration zugeordnet sind. Wenn die interne „`nativ`“ FPolicy Engine verwendet wird, um eine native Dateiblockierungskonfiguration zu erstellen, ist das Erstellen einer externen FPolicy Engine nicht erforderlich.

   Ab ONTAP 9.15.1 kann das `protobuf` Engine-Format verwendet werden. Wenn auf `protobuf` gesetzt, werden die Benachrichtigungsnachrichten binär mit Google Protobuf codiert. Bevor das Engine-Format auf `protobuf` gesetzt wird, ist sicherzustellen, dass der FPolicy Server auch `protobuf` Deserialisierung unterstützt. Weitere Informationen sind unter "Die Konfiguration der externen FPolicy Engine planen" verfügbar.

2. Ein FPolicy Ereignis erstellen.

   Ein FPolicy Ereignis beschreibt, was die FPolicy Richtlinie überwachen soll. Ereignisse bestehen aus den zu überwachenden Protokollen und Dateivorgängen und können eine Liste von Filtern enthalten. Ereignisse verwenden Filter, um die Liste der überwachten Ereignisse einzugrenzen, für die die FPolicy externe Engine Benachrichtigungen senden muss. Ereignisse geben außerdem an, ob die Richtlinie Volumenvorgänge überwacht.

3. Ein persistenter FPolicy Speicher kann erstellt werden (optional).

   Ab ONTAP 9.14.1 ermöglicht FPolicy die Einrichtung von "persistente Speicher" zum Erfassen von Dateizugriffsereignissen für asynchrone, nicht obligatorische Richtlinien in der SVM. Synchrone (obligatorische oder nicht obligatorische) und asynchron obligatorische Konfigurationen werden nicht unterstützt.

   Persistente Speicher können die Client-E/A-Verarbeitung von der FPolicy-Benachrichtigungsverarbeitung entkoppeln, um die Client-Latenz zu reduzieren.

   Ab ONTAP 9.15.1 ist die Konfiguration des persistenten Speichers mit FPolicy vereinfacht. Der `persistent-store-create` Befehl automatisiert die Volume-Erstellung für die SVM und konfiguriert das Volume für den persistenten Store.

4. Eine FPolicy Richtlinie erstellen.

Die FPolicy-Richtlinie ist dafür verantwortlich, dem entsprechenden Geltungsbereich die Menge der zu überwachenden Ereignisse zuzuordnen und festzulegen, für welche der überwachten Ereignisse Benachrichtigungen an den festgelegten FPolicy-Server (oder an die native Engine, falls keine FPolicy-Server konfiguriert sind) gesendet werden müssen. Die Richtlinie definiert außerdem, ob der FPolicy-Server privilegierten Zugriff auf die Daten erhält, für die er Benachrichtigungen empfängt. Ein FPolicy-Server benötigt privilegierten Zugriff, wenn der Server auf die Daten zugreifen muss. Typische Anwendungsfälle, in denen privilegierter Zugriff erforderlich ist, sind Dateisperrung, Quotenverwaltung und hierarchische Speicherverwaltung. In der Richtlinie wird festgelegt, ob die Konfiguration für diese Richtlinie einen FPolicy-Server oder den internen „native“ FPolicy-Server verwendet.

Eine Richtlinie legt fest, ob eine Überprüfung obligatorisch ist. Wenn eine Überprüfung obligatorisch ist und alle FPolicy Server ausgefallen sind oder innerhalb eines definierten Zeitüberschreitung keine Antwort von den FPolicy Servern empfangen wird, wird der Dateizugriff verweigert.

Die Grenzen einer Richtlinie sind die SVM. Eine Richtlinie kann nicht auf mehr als eine SVM angewendet werden. Eine bestimmte SVM kann jedoch mehrere FPolicy Richtlinien haben, die jeweils dieselbe oder unterschiedliche Kombination aus Geltungsbereich, Ereignis und externer Serverkonfiguration aufweisen.

5. Der Richtlinienbereich wird konfiguriert.

   Der FPolicy-Bereich legt fest, auf welche Volumes, Freigaben oder Exportrichtlinien die Richtlinie angewendet wird oder von der Überwachung ausgeschlossen wird. Ein Bereich legt außerdem fest, welche Dateierweiterungen in die FPolicy-Überwachung einbezogen oder von dieser ausgeschlossen werden.

   Ausschlusslisten haben Vorrang vor Einschlusslisten.

6. Die FPolicy Richtlinie wird aktiviert.

   Wenn die Richtlinie aktiviert ist, werden die Kontrollkanäle und optional die privilegierten Datenkanäle verbunden. Der FPolicy Prozess auf den Knoten, an denen die SVM beteiligt ist, beginnt mit der Überwachung des Datei- und Ordnerzugriffs und sendet bei Ereignissen, die den konfigurierten Kriterien entsprechen, Benachrichtigungen an die FPolicy Server (oder an die native Engine, falls keine FPolicy Server konfiguriert sind).

   Wenn die Richtlinie native Dateiblockierung verwendet, ist keine externe Engine konfiguriert oder mit der Richtlinie verknüpft.

Die Konfiguration der externen FPolicy Engine planen

Informationen zur Konfiguration der externen Engine von ONTAP FPolicy

Bevor Sie die externe FPolicy Engine konfigurieren, ist es wichtig zu verstehen, was die Erstellung einer externen Engine bedeutet und welche Konfigurationsparameter verfügbar sind. Diese Informationen unterstützen dabei, die passenden Werte für jeden Parameter festzulegen.

Informationen, die beim Erstellen der externen FPolicy Engine definiert werden

Die externe Engine-Konfiguration definiert die Informationen, die FPolicy benötigt, um Verbindungen zu den externen FPolicy-Servern herzustellen und zu verwalten, einschließlich der folgenden:

- SVM-Name
- Name der Engine
- Die IP-Adressen der primären und sekundären FPolicy Server sowie die TCP-Portnummer, die für die Verbindung zu den FPolicy Servern verwendet wird
- Ob der Engine-Typ asynchron oder synchron ist
- Ob das Engine-Format `xml` oder `protobuf` ist

  Ab ONTAP 9.15.1 kann das `protobuf` Engine-Format verwendet werden. Wenn auf `protobuf` gesetzt, werden die Benachrichtigungsnachrichten binär mit Google Protobuf codiert. Bevor das Engine-Format auf `protobuf` gesetzt wird, ist sicherzustellen, dass der FPolicy Server auch `protobuf` Deserialisierung unterstützt.

  Da das Protobuf-Format ab ONTAP 9.15.1 unterstützt wird, ist das externe Engine-Format zu berücksichtigen, bevor auf eine frühere Version von ONTAP zurückgegangen wird. Bei einer Rückkehr zu einer früheren Version als ONTAP 9.15.1 ist gemeinsam mit dem FPolicy Partner eine der folgenden Optionen zu prüfen:

  - Jedes Engine-Format wird von `protobuf` zu `xml` geändert
  - Die Engines mit einem Engine-Format von `protobuf` löschen
- Authentifizierung der Verbindung zwischen dem Knoten und dem FPolicy Server

  Wenn Sie die gegenseitige SSL-Authentifizierung konfigurieren, müssen auch Parameter konfiguriert werden, die SSL-Zertifikatsinformationen bereitstellen.
- Verwaltung der Verbindung mit verschiedenen erweiterten Berechtigungseinstellungen

  Dies umfasst Parameter, die Dinge wie Zeitüberschreitungswerte, Retry-Werte, Keep-Alive-Werte, maximale Anforderungswerte, Werte für die Größe des Sende- und Empfangspuffers sowie Sitzungs-Zeitüberschreitungswerte definieren.

Der `vserver fpolicy policy external-engine create`Befehl wird verwendet, um eine externe FPolicy Engine zu erstellen.

Was die grundlegenden externen Engine-Parameter sind

Die folgende Tabelle mit grundlegenden FPolicy Konfigurationsparametern kann bei der Planung Ihrer Konfiguration unterstützen:

Art der Information	Option
SVM Gibt den SVM-Namen an, der mit dieser externen Engine verknüpft werden soll. Jede FPolicy Konfiguration ist innerhalb einer einzelnen SVM definiert. Die externe Engine, das Richtlinienereignis, der Richtlinienbereich und die Richtlinie, die zusammen eine FPolicy Richtlinienkonfiguration bilden, müssen alle derselben SVM zugeordnet sein.	`-vserver vserver_name`

Engine-Name Gibt den Namen an, der der externen Engine Konfiguration zugewiesen werden soll. Der Name der externen Engine muss später beim Erstellen der FPolicy Policy angegeben werden. Dadurch wird die externe Engine mit der Policy verknüpft. Der Name darf maximal 256 Zeichen lang sein. Der Name sollte maximal 200 Zeichen lang sein, wenn der Name der externen Engine in einer MetroCluster oder SVM-Disaster-Recovery-Konfiguration konfiguriert wird. Der Name kann jede beliebige Kombination der folgenden ASCII-Zeichen enthalten: • `a`durch `z` • `A`durch `Z` • `0`durch `9` • “_”, “-”, and “.”	`-engine-name engine_name`
Primäre FPolicy Server Gibt die primären FPolicy Server an, an die der Knoten Benachrichtigungen für eine bestimmte FPolicy Richtlinie sendet. Der Wert wird als durch Kommas getrennte Liste von IP-Adressen angegeben. Wenn mehr als eine primäre Server-IP-Adresse angegeben ist, stellt jeder Knoten, an dem die SVM beteiligt ist, zum Zeitpunkt der Aktivierung der Richtlinie eine Steuerverbindung zu jedem angegebenen primären FPolicy Server her. Wenn mehrere primäre FPolicy Server konfiguriert werden, werden Benachrichtigungen im Round-Robin-Verfahren an die FPolicy Server gesendet. Wenn die externe Engine in einer MetroCluster oder SVM-Disaster-Recovery-Konfiguration verwendet wird, sollten die IP-Adressen der FPolicy-Server am Quellstandort als primäre Server angegeben werden. Die IP-Adressen der FPolicy-Server am Zielstandort sollten als sekundäre Server angegeben werden.	`-primary-servers IP_address,...`
Portnummer Gibt die Portnummer des FPolicy Dienstes an.	`-port integer`

Sekundäre FPolicy Server Gibt die sekundären FPolicy-Server an, an die die Dateizugriffsereignisse für eine bestimmte FPolicy-Richtlinie gesendet werden. Der Wert wird als durch Kommas getrennte Liste von IP-Adressen angegeben. Sekundäre Server werden nur verwendet, wenn keiner der primären Server erreichbar ist. Verbindungen zu sekundären Servern werden hergestellt, wenn die Richtlinie aktiviert ist, aber Benachrichtigungen werden nur an sekundäre Server gesendet, wenn keiner der primären Server erreichbar ist. Wenn mehrere sekundäre Server konfiguriert sind, werden Benachrichtigungen im Round-Robin-Verfahren an die FPolicy Server gesendet.	`-secondary-servers IP_address,...`
Externer Engine-Typ Legt fest, ob die externe Engine im synchronen oder asynchronen Modus arbeitet. Standardmäßig arbeitet FPolicy im synchronen Modus. Wenn auf `synchronous` gesetzt, sendet die Dateianforderungsverarbeitung eine Benachrichtigung an den FPolicy Server, wird jedoch erst nach Erhalt einer Antwort vom FPolicy Server fortgesetzt. Zu diesem Zeitpunkt wird der Anforderungsfluss entweder fortgesetzt oder die Verarbeitung führt zu einer Ablehnung, abhängig davon, ob die Antwort des FPolicy Servers die angeforderte Aktion zulässt. Wenn auf `asynchronous` gesetzt, sendet die Dateianforderungsverarbeitung eine Benachrichtigung an den FPolicy Server und wird dann fortgesetzt.	`-extern-engine-type external_engine_type` Der Wert für diesen Parameter kann einer der folgenden sein: • `synchronous` • `asynchronous`
Externes Engine Format Geben Sie an, ob das externe Engine-Format xml oder protobuf ist. Ab ONTAP 9.15.1 kann das Protobuf-Engine-Format verwendet werden. Wenn protobuf ausgewählt ist, werden die Benachrichtigungsnachrichten in binärer Form mit Google Protobuf codiert. Vor dem Einstellen des Engine-Formats auf Protobuf ist sicherzustellen, dass der FPolicy Server ebenfalls die Protobuf-Deserialisierung unterstützt.	`- extern-engine-format` {`protobuf` oder `xml`}

SSL-Option für die Kommunikation mit dem FPolicy Server Legt die SSL-Option für die Kommunikation mit dem FPolicy Server fest. Dies ist ein Pflichtparameter. Eine der Optionen kann anhand der folgenden Informationen ausgewählt werden: • Wenn auf `no-auth` gesetzt, findet keine Authentifizierung statt. Die Kommunikationsverbindung wird über TCP hergestellt. • Wenn diese Option auf `server-auth` gesetzt ist, authentifiziert die SVM den FPolicy Server mittels SSL-Authentifizierung. • Wenn auf `mutual-auth` gesetzt, findet eine gegenseitige Authentifizierung zwischen der SVM und dem FPolicy Server statt; die SVM authentifiziert den FPolicy Server und der FPolicy Server authentifiziert die SVM. Wenn Sie die gegenseitige SSL-Authentifizierung konfigurieren, müssen Sie auch die `-certificate-common-name`, `-certificate -serial` und `-certifcate-ca` Parameter konfigurieren.	`-ssl-option` {`no-auth`
`server-auth`	`mutual-auth`}
FQDN des Zertifikats oder benutzerdefinierter allgemeiner Name Gibt den Zertifikatsnamen an, der verwendet wird, wenn die SSL-Authentifizierung zwischen der SVM und dem FPolicy Server konfiguriert ist. Der Zertifikatsname kann als FQDN oder als benutzerdefinierter allgemeiner Name angegeben werden. Wenn Sie `mutual-auth` für den `-ssl-option` Parameter angeben, muss ein Wert für den `-certificate-common-name` Parameter angegeben werden.	`-certificate-common -name text`
Seriennummer des Zertifikats Gibt die Seriennummer des Zertifikats an, das für die Authentifizierung verwendet wird, wenn eine SSL-Authentifizierung zwischen der SVM und dem FPolicy Server konfiguriert ist. Wenn Sie `mutual-auth` für den `-ssl-option` Parameter angeben, muss ein Wert für den `-certificate-serial` Parameter angegeben werden.	`-certificate-serial text`
Zertifizierungsstelle Gibt den CA-Namen des Zertifikats an, das für die Authentifizierung verwendet wird, wenn eine SSL-Authentifizierung zwischen der SVM und dem FPolicy Server konfiguriert ist. Wenn Sie `mutual-auth` für den `-ssl-option` Parameter angeben, muss ein Wert für den `-certificate-ca` Parameter angegeben werden.	`-certificate-ca text`

Was die erweiterten externen Engine-Optionen sind

Die folgende Tabelle mit erweiterten FPolicy-Konfigurationsparametern bietet eine Übersicht, um zu

entscheiden, ob die Konfiguration mit erweiterten Parametern angepasst werden soll. Diese Parameter dienen zur Anpassung des Kommunikationsverhaltens zwischen den Cluster-Knoten und den FPolicy Servern:

Art der Information	Option
Zeitüberschreitung beim Abbrechen einer Anfrage Gibt das Zeitintervall in Stunden (`h`), Minuten (`m`) oder Sekunden (`s`) an, das der Knoten auf eine Antwort vom FPolicy Server wartet. Läuft das Zeitüberschreitungsintervall ab, sendet der Knoten eine Abbruchanfrage an den FPolicy Server. Anschließend sendet der Knoten die Benachrichtigung an einen alternativen FPolicy Server. Diese Zeitüberschreitung hilft bei der Behandlung eines nicht reagierenden FPolicy Servers, was die Antwortzeiten von SMB/NFS-Clients verbessern kann. Auch das Abbrechen von Anfragen nach einer Zeitüberschreitung kann zur Freigabe von Systemressourcen beitragen, da die Benachrichtigungsanfrage von einem ausgefallenen oder fehlerhaften FPolicy Server an einen alternativen FPolicy Server verschoben wird. Der Wertebereich für diesen Wert ist `0` bis `100`. Wenn der Wert auf `0` gesetzt ist, ist die Option deaktiviert und Abbruchanforderungen werden nicht an den FPolicy Server gesendet. Der Standardwert ist `20s`.	`-reqs-cancel-timeout integer`[h
m	s]
Zeitüberschreitung beim Abbruch einer Anfrage Gibt die Zeitüberschreitung in Stunden (`h`), Minuten (`m`) oder Sekunden (`s`) für den Abbruch einer Anfrage an. Der Wertebereich für diesen Wert ist `0` bis `200`.	`-reqs-abort-timeout ` `integer`[h
m	s]
Intervall für das Senden von Statusanfragen Gibt das Intervall in Stunden (`h`), Minuten (`m`) oder Sekunden (`s`) an, nach dem eine Statusanfrage an den FPolicy Server gesendet wird. Der Wertebereich für diesen Wert ist `0` bis `50`. Wenn der Wert auf `0` gesetzt ist, ist die Option deaktiviert und Statusanforderungsmeldungen werden nicht an den FPolicy Server gesendet. Der Standardwert ist `10s`.	`-status-req-interval integer`[h
m	s]
Maximale Anzahl ausstehender Anfragen auf dem FPolicy Server Gibt die maximale Anzahl ausstehender Anfragen an, die auf dem FPolicy Server in die Warteschlange gestellt werden können. Der Wertebereich für diesen Wert ist `1` bis `10000`. Der Standardwert ist `500`.	`-max-server-reqs integer`

Zeitüberschreitung beim Trennen der Verbindung zu einem nicht reagierenden FPolicy Server Gibt das Zeitintervall in Stunden (`h`), Minuten (`m`) oder Sekunden (`s`) an, nach dem die Verbindung zum FPolicy Server beendet wird. Die Verbindung wird nach Ablauf der Zeitüberschreitungsperiode nur dann getrennt, wenn die Warteschlange des FPolicy-Servers die maximal zulässige Anzahl an Anfragen enthält und innerhalb der Zeitüberschreitungsperiode keine Antwort empfangen wird. Die maximal zulässige Anzahl an Anfragen ist entweder `50` (der Standardwert) oder die durch den `max-server-reqs-` Parameter festgelegte Anzahl. Der Wertebereich für diesen Wert ist `1` bis `100`. Der Standardwert ist `60s`.	`-server-progress -timeout integer`[h
m	s]
Intervall für das Senden von Keep-Alive-Nachrichten an den FPolicy Server Gibt das Zeitintervall in Stunden (`h`), Minuten (`m`) oder Sekunden (`s`) an, in dem Keep-Alive-Nachrichten an den FPolicy Server gesendet werden. Keep-alive-Nachrichten erkennen halbgeöffnete Verbindungen. Der Wertebereich für diesen Wert ist `10` bis `600`. Wenn der Wert auf `0` gesetzt ist, ist die Option deaktiviert und Keep-Alive-Nachrichten werden nicht an die FPolicy Server gesendet. Der Standardwert ist `120s`.	`-keep-alive-interval-integer`[h
m	s]
Maximale Anzahl an Wiederverbindungsversuchen Legt die maximale Anzahl der Versuche fest, die die SVM unternimmt, um die Verbindung zum FPolicy Server wiederherzustellen, nachdem die Verbindung unterbrochen wurde. Der Wertebereich für diesen Wert ist `0` bis `20`. Der Standardwert ist `5`.	`-max-connection-retries integer`
Empfangspuffergröße Legt die Empfangspuffergröße des verbundenen Sockets für den FPolicy Server fest. Der Standardwert ist auf 256 Kilobyte (Kb) eingestellt. Wenn der Wert auf 0 gesetzt ist, wird die Größe des Empfangspuffers auf einen vom System definierten Wert festgelegt. Wenn beispielsweise die Standardgröße des Empfangspuffers des Sockets 65536 Byte beträgt, wird durch Setzen des einstellbaren Werts auf 0 die Socket-Puffergröße auf 65536 Byte festgelegt. Jeder Wert ungleich dem Standardwert kann verwendet werden, um die Größe (in Byte) des Empfangspuffers festzulegen.	`-recv-buffer-size integer`

Sendepuffergröße Legt die Größe des Sendepuffers des verbundenen Sockets für den FPolicy Server fest. Der Standardwert ist auf 256 Kilobyte (Kb) eingestellt. Wenn der Wert auf 0 gesetzt ist, wird die Größe des Sendepuffers auf einen vom System definierten Wert festgelegt. Wenn beispielsweise die Standardgröße des Sendepuffers des Sockets auf 65536 Byte festgelegt ist, wird durch Setzen des anpassbaren Werts auf 0 die Socket-Puffergröße auf 65536 Byte eingestellt. Jeder Wert ungleich dem Standardwert kann verwendet werden, um die Größe (in Byte) des Sendepuffers festzulegen.	`-send-buffer-size integer`
Zeitüberschreitung beim Löschen einer Sitzungs-ID während der Wiederverbindung Gibt das Intervall in Stunden (`h`), Minuten (`m`) oder Sekunden (`s`) an, nach dem bei Wiederverbindungsversuchen eine neue Sitzungs-ID an den FPolicy Server gesendet wird. Wird die Verbindung zwischen dem Storage Controller und dem FPolicy Server unterbrochen und innerhalb des `-session-timeout` Intervalls wiederhergestellt, wird die alte Sitzungs-ID an den FPolicy Server gesendet, damit dieser Antworten auf alte Benachrichtigungen senden kann. Der Standardwert ist auf 10 Sekunden eingestellt.	`-session-timeout [integerh][integerm][integers]`

Wie externe ONTAP FPolicy-Engines SSL-authentifizierte Verbindungen verwenden

Einige zusätzliche Informationen sind erforderlich, wenn die externe FPolicy Engine für die Verwendung von SSL bei der Verbindung mit FPolicy Servern konfiguriert werden soll.

SSL-Serverauthentifizierung

Wenn Sie die externe FPolicy Engine für die SSL-Serverauthentifizierung konfigurieren, muss vor der Erstellung der externen Engine das öffentliche Zertifikat der Zertifizierungsstelle (CA), die das FPolicy Serverzertifikat signiert hat, installiert werden.

Gegenseitige Authentifizierung

Wenn externe FPolicy Engines so konfiguriert werden, dass sie bei der Verbindung von Storage Virtual Machine (SVM) Daten-LIFs mit externen FPolicy Servern die gegenseitige SSL Authentifizierung verwenden, muss vor der Erstellung der externen Engine das öffentliche Zertifikat der CA, die das FPolicy Serverzertifikat signiert hat, zusammen mit dem öffentlichen Zertifikat und der Schlüsseldatei für die Authentifizierung der SVM installiert werden. Dieses Zertifikat darf nicht gelöscht werden, solange FPolicy Richtlinien das installierte Zertifikat verwenden.

Wird das Zertifikat gelöscht, während FPolicy es für die gegenseitige Authentifizierung bei der Verbindung zu einem externen FPolicy Server verwendet, kann eine deaktivierte FPolicy Richtlinie, die dieses Zertifikat nutzt, nicht wieder aktiviert werden. Die FPolicy Richtlinie kann in diesem Fall auch dann nicht reaktiviert werden, wenn ein neues Zertifikat mit denselben Einstellungen erstellt und auf der SVM installiert wird.

Wenn das Zertifikat gelöscht wurde, ist ein neues Zertifikat zu installieren, neue FPolicy externe Engines zu erstellen, die das neue Zertifikat verwenden, und die neuen externen Engines der FPolicy Richtlinie zuzuordnen, die durch Ändern der FPolicy Richtlinie wieder aktiviert werden soll.

Zertifikate für SSL installieren

Das öffentliche Zertifikat der Zertifizierungsstelle, das zum Signieren des FPolicy Serverzertifikats verwendet wird, wird mit dem `security certificate install` Befehl und dem `-type` Parameter, der auf `client-ca` gesetzt ist, installiert. Der für die Authentifizierung der SVM erforderliche private Schlüssel und das öffentliche Zertifikat werden mit dem `security certificate install` Befehl und dem `-type` Parameter, der auf `server` gesetzt ist, installiert.

Verwandte Informationen

- "Sicherheitszertifikat installieren"

ONTAP FPolicy Zertifikatreplikation bei SVM Notfallwiederherstellung ohne ID-Erhaltung

Die für die SSL-Authentifizierung bei Verbindungen zu FPolicy Servern verwendeten Sicherheitszertifikate werden nicht auf SVM Disaster Recovery-Ziele mit Konfigurationen ohne ID-Erhaltung repliziert. Obwohl die FPolicy External-Engine-Konfiguration auf der SVM repliziert wird, werden die Sicherheitszertifikate nicht repliziert. Die Sicherheitszertifikate müssen manuell auf dem Ziel installiert werden.

Wenn Sie die SVM-Notfallwiederherstellungsbeziehung einrichten, bestimmt der Wert, den Sie für die `-identity-preserve` Option des `snapmirror create` Befehls auswählen, die Konfigurationsdetails, die in die Ziel-SVM repliziert werden.

Wenn die `-identity-preserve` Option auf `true` (ID-preserve) gesetzt ist, werden alle FPolicy-Konfigurationsdetails einschließlich der Informationen zum Sicherheitszertifikat repliziert. Die Sicherheitszertifikate müssen nur auf dem Ziel installiert werden, wenn die Option auf `false` (non-ID-preserve) gesetzt ist.

Verwandte Informationen

- "snapmirror create"

Einschränkungen für externe FPolicy-Engines mit MetroCluster und SVM-Notfallwiederherstellung in ONTAP

Sie können eine clusterweite externe FPolicy-Engine erstellen, indem Sie die Cluster-Speicher-VM (SVM) der externen Engine zuweisen. Bei der Erstellung einer clusterweiten externen Engine in einer MetroCluster oder SVM-Disaster-Recovery-Konfiguration bestehen jedoch bestimmte Einschränkungen bei der Auswahl des Authentifizierungsverfahrens, das die SVM für die externe Kommunikation mit dem FPolicy-Server verwendet.

Es stehen drei Authentifizierungsoptionen zur Auswahl, wenn externe FPolicy-Server erstellt werden: keine Authentifizierung, SSL-Serverauthentifizierung und SSL-Gegenseitige Authentifizierung. Obwohl bei der Auswahl der Authentifizierungsoption keine Einschränkungen bestehen, wenn der externe FPolicy-Server einer Daten-SVM zugewiesen ist, gibt es Einschränkungen beim Erstellen einer FPolicy-Engine mit Cluster-Umfang:

Konfiguration	Gestattet?
MetroCluster oder SVM-Notfallwiederherstellung und eine clusterweite externe FPolicy Engine ohne Authentifizierung (SSL ist nicht konfiguriert)	Ja
MetroCluster oder SVM-Notfallwiederherstellung und eine clusterweite externe FPolicy Engine mit SSL-Server oder gegenseitiger SSL-Authentifizierung	Nein

- Wenn eine FPolicy-Engine mit Cluster-Bezug und externer Engine sowie SSL-Authentifizierung vorhanden ist und eine MetroCluster oder SVM Disaster Recovery-Konfiguration erstellt werden soll, muss diese externe Engine so geändert werden, dass keine Authentifizierung verwendet wird, oder die externe Engine muss entfernt werden, bevor die MetroCluster oder SVM Disaster Recovery-Konfiguration erstellt werden kann.
- Wenn die MetroCluster oder SVM-Notfallwiederherstellungskonfiguration bereits existiert, verhindert ONTAP die Erstellung einer clusterweiten FPolicy externen Engine mit SSL-Authentifizierung.

ONTAP FPolicy Konfigurationsarbeitsblätter für externe Engines

Sie können dieses Arbeitsblatt verwenden, um die Werte zu erfassen, die Sie während des FPolicy External Engine Konfigurationsprozesses benötigen. Falls ein Parameterwert erforderlich ist, sollte vor der Konfiguration der External Engine festgelegt werden, welcher Wert für diese Parameter zu verwenden ist.

Informationen für eine grundlegende externe Engine-Konfiguration

Es empfiehlt sich, festzuhalten, ob jede Parametereinstellung in die externe Engine Konfiguration aufgenommen werden soll, und anschließend den Wert der Parameter zu notieren, die aufgenommen werden sollen.

Art der Information	Erforderlich	Enthalten	Ihre Werte
Name der Storage Virtual Machine (SVM)	Ja	Ja	
Name der Engine	Ja	Ja	
Primäre FPolicy Server	Ja	Ja	
Portnummer	Ja	Ja	
Sekundäre FPolicy Server	Nein		
Externer Engine-Typ	Nein		
SSL Option für die Kommunikation mit dem externen FPolicy Server	Ja	Ja	
Zertifikat FQDN oder benutzerdefinierter allgemeiner Name	Nein		
Zertifikatsseriennummer	Nein		
Zertifizierungsstelle	Nein		

Informationen zu erweiterten externen Engine-Parametern

Um eine externe Engine mit erweiterten Parametern zu konfigurieren, ist der Konfigurationsbefehl im erweiterten Berechtigungsmodus einzugeben.

Art der Information	Erforderlich	Enthalten	Ihre Werte
Zeitüberschreitung beim Abbrechen einer Anfrage	Nein		
Zeitüberschreitung beim Abbruch einer Anfrage	Nein		
Intervall für das Senden von Statusanfragen	Nein		
Maximale Anzahl ausstehender Anfragen auf dem FPolicy Server	Nein		
Zeitüberschreitung beim Trennen der Verbindung zu einem nicht reagierenden FPolicy Server	Nein		
Intervall für das Senden von Keep-Alive-Nachrichten an den FPolicy Server	Nein		
Maximale Anzahl an Wiederverbindungsversuchen	Nein		
Empfangspuffergröße	Nein		
Sendepuffergröße	Nein		
Zeitüberschreitung beim Löschen einer Sitzungs-ID während der Wiederverbindung	Nein		

Die FPolicy Ereigniskonfiguration planen

Informationen zur ONTAP FPolicy Ereigniskonfiguration

Bevor Sie FPolicy-Ereignisse konfigurieren, ist es wichtig zu verstehen, was es bedeutet, ein FPolicy-Ereignis zu erstellen. Es sollte festgelegt werden, welche Protokolle das Ereignis überwachen soll, welche Ereignisse überwacht werden und welche Ereignisfilter verwendet werden. Diese Informationen unterstützen die Planung der gewünschten Werte.

Was es bedeutet, ein FPolicy Ereignis zu erstellen

Das Erstellen eines FPolicy-Ereignisses bedeutet, Informationen zu definieren, die der FPolicy-Prozess benötigt, um zu bestimmen, welche Dateizugriffsvorgänge überwacht werden sollen und welche Benachrichtigungen über die überwachten Ereignisse an den externen FPolicy-Server gesendet werden sollen. Die FPolicy-Ereigniskonfiguration definiert die folgenden Konfigurationsinformationen:

- Name der Storage Virtual Machine (SVM)
- Veranstaltungsname
- Zu überwachende Protokolle

  FPolicy kann Dateizugriffsvorgänge über SMB, NFSv3, NFSv4, NFSv4.1 (ab ONTAP 9.15.1) und S3 (ab ONTAP 9.20.1) überwachen.

- Welche Dateivorgänge überwacht werden sollen

Nicht alle Dateivorgänge sind für jedes Protokoll gültig.

- Welche Dateifilter konfiguriert werden sollten

  Nur bestimmte Kombinationen von Dateivorgängen und Filtern sind gültig. Jedes Protokoll hat seine eigene Menge an unterstützten Kombinationen.

- Ob die Ein- und Aushängevorgänge von Datenträgern überwacht werden

> Es besteht eine Abhängigkeit zwischen drei der Parameter (`-protocol`, `-file-operations`, `-filters`). Die folgenden Kombinationen sind für die drei Parameter gültig:
>
> - Sie können die `-protocol` und `-file-operations` Parameter angeben.
> - Sie können alle drei Parameter angeben.
> - Es kann keiner der Parameter angegeben werden.

Was die FPolicy Ereigniskonfiguration enthält

Die folgende Liste der verfügbaren FPolicy Ereigniskonfigurationsparameter kann bei der Planung der Konfiguration unterstützen:

Art der Information	Option
SVM Gibt den SVM Namen an, der mit diesem FPolicy Ereignis verknüpft werden soll. Jede FPolicy Konfiguration ist innerhalb einer einzelnen SVM definiert. Die externe Engine, das Richtlinienereignis, der Richtlinienbereich und die Richtlinie, die zusammen eine FPolicy Richtlinienkonfiguration bilden, müssen alle derselben SVM zugeordnet sein.	`-vserver vserver_name`

Ereignisname Gibt den Namen an, der dem FPolicy-Ereignis zugewiesen werden soll. Beim Erstellen der FPolicy Richtlinie wird das FPolicy Ereignis der Richtlinie anhand des Ereignisnamens zugeordnet. Der Name darf maximal 256 Zeichen lang sein. Der Name darf maximal 200 Zeichen lang sein, wenn das Ereignis 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 “.”	`-event-name event_name`
Protokoll Gibt an, welches Protokoll für das FPolicy-Ereignis konfiguriert werden soll. Die Liste für `-protocol` kann einen der folgenden Werte enthalten: • `cifs` • `nfsv3` • `nfsv4` • `nfsv4.1` (beginnend mit ONTAP 9.15.1) • `s3`(ab ONTAP 9.20.1) Wenn `-protocol` angegeben wird, muss ein gültiger Wert im `-file-operations` Parameter angegeben werden. Mit Änderungen an der Protokollversion können sich die gültigen Werte ändern.	`-protocol protocol`

Dateioperationen Gibt die Liste der Dateivorgänge für das FPolicy Ereignis an. Das Ereignis prüft die in dieser Liste aufgeführten Operationen aller Clientanfragen, die das im `-protocol` Parameter angegebene Protokoll verwenden. Eine oder mehrere Dateioperationen können als kommagetrennte Liste aufgeführt werden. Die Liste für `-file -operations` kann einen oder mehrere der folgenden Werte enthalten: • `close` für Dateischließungsvorgänge • `create` für Dateierstellungsvorgänge • `create-dir` für Verzeichniserstellungsoperationen • `delete` für Dateilöschvorgänge • `delete_dir` für Verzeichnislöschvorgänge • `getattr` für Attributabrufoperationen • `link` für Link-Operationen • `lookup` für Suchvorgänge • `object_create` für S3-Dateioperationen • `object_delete` für S3-Dateioperationen • `object_tag` für S3-Dateivorgänge • `open` für Dateiöffnungsvorgänge • `read` für Dateileseoperationen • `write` für Dateischreibvorgänge • `rename` für Dateiumbenennungsvorgänge • `rename_dir` für Verzeichnisumbenennungsvorgänge • `setattr` für Set-Attribut-Operationen • `symlink` für Symbol-Link-Operationen Wenn `-file-operations` angegeben wird, muss im `-protocol` Parameter ein gültiges Protokoll angegeben werden.	`-file-operations file_operations,...`

Filter Gibt die Liste der Filter für eine bestimmte Dateioperation für das angegebene Protokoll an. Die Werte im `-filters` Parameter werden verwendet, um Clientanfragen zu filtern. Die Liste kann einen oder mehrere der folgenden enthalten: Wenn Sie den `-filters` Parameter angeben, müssen Sie auch gültige Werte für die `-file-operations` und `-protocol` Parameter angeben. • `close-with-modification`Option zum Filtern der Client-Anfrage zum Schließen mit Änderung. • `close-without-modification`Option zum Filtern der Client-Anfrage zum Schließen ohne Änderung. • `first-read`Option zum Filtern der Client-Anfrage für den ersten Lesevorgang. • `first-write` Option zum Filtern der Clientanfrage für den ersten Schreibvorgang. • `monitor-ads`Option zum Filtern der Clientanfrage nach alternativem Datenstrom. • `object-create-with-put` Option zum Filtern von S3-Objekten. • `object-create-with-copy` Option zum Filtern von S3-Objekten. • `object-create-with-complete-mpu` Option zum Filtern von S3-Objekten. • `exclude-multi-delete` Option zum Filtern von S3-Objekten. • `object-tag-put` Option zum Filtern von S3-Objekten. • `object-tag-delete` Option zum Filtern von S3-Objekten. • `offline-bit`Option zum Filtern der Clientanfrage nach gesetztem Offline-Bit. Durch das Setzen dieses Filters erhält der FPolicy Server nur dann eine Benachrichtigung, wenn auf Offline-Dateien zugegriffen wird. • `open-with-delete-intent`Option zum Filtern der Client-Anfrage für das Öffnen mit Löschabsicht. Durch Aktivieren dieses Filters erhält der FPolicy-Server nur dann eine Benachrichtigung, wenn versucht wird, eine Datei mit der Absicht zu öffnen, sie zu löschen. Dies wird von Dateisystemen verwendet, wenn das `FILE_DELETE_ON_CLOSE` Flag angegeben ist. • `open-with-write-intent`Option zum Filtern von Client-Requests zum Öffnen mit Schreibabsicht. Durch die Einstellung dieses Filters erhält der FPolicy Server nur dann eine Benachrichtigung, wenn versucht wird, eine Datei mit der Absicht	`-filters filter, ...`

Ist ein Volume-Vorgang erforderlich? Gibt an, ob die Überwachung von Volume-Mount- und Unmount-Vorgängen erforderlich ist. Der Standardwert ist `false`.	`-volume-operation {true`

`false}`
 	
`-filters filter, ...`
	FPolicy-Zugriff verweigert Benachrichtigungen
	
	Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen über fehlgeschlagene Dateivorgänge aufgrund fehlender Berechtigungen erhalten. Diese Benachrichtigungen sind wertvoll für Sicherheit, Ransomware-Schutz und Governance. Benachrichtigungen werden für fehlgeschlagene Dateivorgänge aufgrund fehlender Berechtigungen generiert, darunter:
	
	• Fehler aufgrund von NTFS-Berechtigungen.
	• Fehler aufgrund von Unix-Modusbits.
	• Fehler aufgrund von NFSv4 ACLs.

`-monitor-fileop-failure {true`	`false}`

Unterstützte FPolicy Dateioperationen und Filter für SMB in ONTAP

Bei der Konfiguration Ihres FPolicy-Ereignisses ist zu beachten, dass nur bestimmte Kombinationen von Dateioperationen und Filtern für die Überwachung von SMB-Dateizugriffsvorgängen unterstützt werden.

Die Liste der unterstützten Dateioperationen- und Filterkombinationen für die FPolicy Überwachung von SMB-Dateizugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützte Dateivorgänge	Unterstützte Filter
schließen	monitor-ads, offline-bit, close-with-modification, close-without-modification, close-with-read, exclude-directory
erstellen	monitor-ads, offline-bit
Verzeichnis erstellen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
löschen	monitor-ads, offline-bit
Verzeichnis löschen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
getattr	offline-Bit, exclude-dir

offen	monitor-ads, offline-bit, open-with-delete-intent, open-with-write-intent, exclude-dir
lesen	monitor-ads, offline-bit, first-read
schreiben	monitor-ads, offline-bit, first-write, write-with-size-change
umbenennen	monitor-ads, offline-bit
Verzeichnis umbenennen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
setattr	monitor-ads, offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_creation_time_change, setattr_with_size_change, setattr_with_allocation_size_change, exclude_directory

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen über fehlgeschlagene Dateivorgänge aufgrund fehlender Berechtigungen erhalten. Die Liste der unterstützten Kombinationen aus verweigerten Dateizugriffsvorgängen und Filtern für die FPolicy Überwachung von SMB Dateizugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützte Datei-Zugriffsverweigerungsoperation	Unterstützte Filter
offen	NA

Unterstützte FPolicy Dateioperationen und Filter für NFSv3 in ONTAP

Bei der Konfiguration Ihres FPolicy Ereignisses ist zu beachten, dass für die Überwachung von NFSv3-Dateizugriffsvorgängen nur bestimmte Kombinationen von Dateivorgängen und Filtern unterstützt werden.

Die Liste der unterstützten Dateioperationen- und Filterkombinationen für die FPolicy Überwachung von NFSv3-Dateizugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützte Dateivorgänge	Unterstützte Filter
erstellen	Offline Bit
Verzeichnis erstellen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
löschen	Offline Bit
Verzeichnis löschen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
Link	Offline Bit
Nachschlagen	offline-Bit, exclude-dir
lesen	Offline-Bit, First-Read
schreiben	offline-bit, First-Write, Write-with-Size-Change
umbenennen	Offline Bit
Verzeichnis umbenennen	Aktuell wird für diese Dateioperation kein Filter unterstützt.

setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
Symlink	Offline Bit

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen über fehlgeschlagene Dateivorgänge aufgrund fehlender Berechtigungen erhalten. Die Liste der unterstützten Kombinationen aus verweigertem Dateizugriff und Filter für die FPolicy Überwachung von NFSv3 Dateizugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützte Datei-Zugriffsverweigerungsoperation	Unterstützte Filter
Zugriff	NA
erstellen	NA
Verzeichnis erstellen	NA
löschen	NA
Verzeichnis löschen	NA
Link	NA
lesen	NA
umbenennen	NA
Verzeichnis umbenennen	NA
setattr	NA
schreiben	NA

Unterstützte FPolicy Dateioperationen und Filter für NFSv4 in ONTAP

Bei der Konfiguration Ihres FPolicy Ereignisses ist zu beachten, dass für die Überwachung von NFSv4-Dateizugriffsvorgängen nur bestimmte Kombinationen von Dateivorgängen und Filtern unterstützt werden.

Ab ONTAP 9.15.1 unterstützt FPolicy das NFSv4.1 Protokoll.

Ab ONTAP 9.19.1 können Administratoren die Verfügbarkeit von NFSv4.2 auf SVM-Ebene steuern, indem sie das Protokoll für einzelne Storage-VMs entweder über System Manager, die CLI oder REST API aktivieren oder deaktivieren.

Ab ONTAP 9.20.1 unterstützt FPolicy die Überwachung von NFSv4.2-Dateizugriffsereignissen, einschließlich neuer Dateivorgänge für Schreibvorgänge mit erweiterten Attributen (xattr) und Sicherheitslabelfiltern für Labeled NFS-Aktivitäten. Weitere Informationen zu "NFS für ONTAP SVMs aktivieren oder deaktivieren".

> Sicherheitslabel-Filter (`setattr_with_security_label_change` und `getattr_with_security_label_read`) erfordern, dass NFSv4.2-Sicherheitslabels (Labeled NFS) auf der SVM aktiviert sind. Weitere Informationen zu "Aktivierung von NFSv4.2 Sicherheitskennzeichnungen". `getxattr` und `listxattrs` sind schreibgeschützte Operationen und werden nicht von FPolicy überwacht.

Die Liste der unterstützten Dateioperations- und Filterkombinationen für die FPolicy-Überwachung von Dateizugriffsereignissen in NFSv4, NFSv4.1 oder NFSv4.2 ist in der folgenden Tabelle aufgeführt:

Unterstützte Dateivorgänge	Unterstützte Filter
schließen	Offline-Bit, exclude-directory
erstellen	Offline Bit
Verzeichnis erstellen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
löschen	Offline Bit
Verzeichnis löschen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
getattr	offline-bit, exclude-directory getattr_with_security_label_read (Ab ONTAP 9.20.1 ist dieser Filter verfügbar, Labeled NFS ist erforderlich)
Link	Offline Bit
Nachschlagen	Offline-Bit, exclude-directory
offen	Offline-Bit, exclude-directory
lesen	Offline-Bit, First-Read
schreiben	offline-bit, First-Write, Write-with-Size-Change
umbenennen	Offline Bit
Verzeichnis umbenennen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory setattr_with_security_label_change (ab ONTAP 9.20.1 unterstützt ONTAP diesen Filter; Voraussetzung ist Labeled NFS)
setxattr	Ab ONTAP 9.20.1 wird dieser Dateivorgang unterstützt und erfordert Labeled NFS. Derzeit wird für diesen Dateivorgang kein Filter unterstützt.
removexattr	Ab ONTAP 9.20.1 wird dieser Dateivorgang unterstützt und erfordert Labeled NFS. Derzeit wird für diesen Dateivorgang kein Filter unterstützt.
Symlink	Offline Bit

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen über fehlgeschlagene Dateivorgänge aufgrund fehlender Berechtigungen erhalten. Die Liste der unterstützten Kombinationen aus Zugriffsverweigerung bei Dateivorgängen und Filtern für die FPolicy-Überwachung von Dateizugriffsereignissen in NFSv4, NFSv4.1 oder NFSv4.2 ist in der folgenden Tabelle aufgeführt:

Unterstützte Datei-Zugriffsverweigerungsoperation	Unterstützte Filter
Zugriff	k. A.
erstellen	k. A.
Verzeichnis erstellen	k. A.
löschen	k. A.
Verzeichnis löschen	k. A.
Link	k. A.

offen	k. A.
lesen	k. A.
umbenennen	k. A.
Verzeichnis umbenennen	k. A.
setattr	k. A.
schreiben	k. A.

Unterstützte Dateioperationen- und Filterkombinationen, die ONTAP FPolicy für S3 überwacht

Bei der Konfiguration Ihres FPolicy-Ereignisses ist zu beachten, dass für die Überwachung von S3-Objektzugriffsvorgängen nur bestimmte Kombinationen von Dateivorgängen und Filtern unterstützt werden.

Ab ONTAP 9.20.1 unterstützt FPolicy Benachrichtigungen für S3-Objektereignisse auf NAS-Buckets. S3 FPolicy arbeitet ausschließlich im asynchronen, nicht obligatorischen Modus.

Die Liste der unterstützten Dateivorgänge und Filterkombinationen für die FPolicy Überwachung von S3-Objektzugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützte Dateivorgänge	Unterstützte Filter
object_create	object-create-with-put, object-create-with-copy, object-create-with-complete-mpu
object_delete	exclude-multi-delete
object_tag	object-tag-put, object-tag-delete

Filterbeschreibungen

Die folgende Liste beschreibt jeden S3 FPolicy-Filter:

- object-create-with-put: Überwachung von Objekterstellungsvorgängen, die mithilfe einer PUT-Anfrage durchgeführt werden.
- object-create-with-copy: Überwachung von Objekterstellungsvorgängen, die mit einer COPY-Anforderung durchgeführt werden.
- object-create-with-complete-mpu: Überwachung von Objekterstellungsvorgängen, die durch das Abschließen eines Multipart-Uploads ausgeführt werden.
- Mehrfachlöschung ausschließen: Benachrichtigungen für Objekte, die im Rahmen einer Mehrfachlöschungsanforderung gelöscht wurden, werden ausgeschlossen. Wenn dieser Filter aktiviert ist, generiert FPolicy nur Benachrichtigungen für Löschvorgänge einzelner Objekte.
- object-tag-put: Überwachung von Vorgängen, die ein Objekt-Tag hinzufügen oder ändern.
- object-tag-delete: Überwachung von Vorgängen, die ein Objekt-Tag entfernen.

Zusätzliche Überlegungen zu S3 FPolicy Ereignissen

- Nur erfolgreiche, clientgesteuerte S3-Operationen generieren FPolicy-Benachrichtigungen. Intern generierte Operationen (wie z. B. Objektablauf oder Snapshot-Wiederherstellung) und fehlgeschlagene Operationen generieren keine Benachrichtigungen.

- GET-Operationen (Lesen) werden für die S3 FPolicy Überwachung nicht unterstützt.
- Eine Mehrfachlöschanforderung kann bis zu 1.000 Objekte löschen. FPolicy generiert für jedes erfolgreich gelöschte Objekt eine Benachrichtigung. Jede Benachrichtigung innerhalb derselben Mehrfachlöschanforderung verwendet dieselbe FPolicy Anforderungs-ID und S3 Anforderungs-ID zur Korrelation.
- Benachrichtigungen über verweigerten Zugriff werden für S3-Ereignisse nicht unterstützt.

ONTAP FPolicy Ereigniskonfigurationsarbeitsblatt

Sie können dieses Arbeitsblatt verwenden, um die Werte zu erfassen, die Sie während des FPolicy Ereignis-Konfigurationsprozesses benötigen. Wenn ein Parameterwert erforderlich ist, muss vor der Konfiguration des FPolicy Ereignisses festgelegt werden, welcher Wert für diese Parameter zu verwenden ist.

Es empfiehlt sich, festzuhalten, ob jede Parametereinstellung in die FPolicy Ereigniskonfiguration aufgenommen werden soll, und anschließend den Wert der Parameter zu notieren, die aufgenommen werden sollen.

Art der Information	Erforderlich	Enthalten	Ihre Werte
Name der Storage Virtual Machine (SVM)	Ja	Ja	
Veranstaltungsname	Ja	Ja	
Protokoll	Nein		
Dateivorgänge	Nein		
Filter	Nein		
Volume-Betrieb	Nein		
Zugriffsverweigerungsereignisse + (Unterstützung ab ONTAP 9.13)	Nein		

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?		

Planung der FPolicy Bereichskonfiguration

Informationen zu den Bereichskonfigurationen von ONTAP FPolicy

Bevor Sie den FPolicy-Bereich konfigurieren, müssen Sie verstehen, was die Erstellung eines Bereichs bedeutet. Sie müssen verstehen, was die Bereichskonfiguration enthält. Sie müssen außerdem wissen, welche Vorrangregeln für den Bereich gelten. Diese Informationen können bei der Planung der Werte, die Sie festlegen möchten, helfen.

Was es bedeutet, einen FPolicy Bereich zu erstellen

Die Erstellung des FPolicy-Bereichs bedeutet, die Grenzen festzulegen, auf die die FPolicy-Richtlinie angewendet wird. Die Storage Virtual Machine (SVM) ist die grundlegende Grenze. Beim Erstellen eines Bereichs für eine FPolicy-Richtlinie ist die FPolicy-Richtlinie zu definieren, auf die er angewendet wird, und es ist anzugeben, auf welche SVM der Bereich angewendet werden soll.

Es gibt eine Reihe von Parametern, die den Geltungsbereich innerhalb der angegebenen SVM weiter einschränken. Der Geltungsbereich kann eingeschränkt werden, indem festgelegt wird, was in den Geltungsbereich einbezogen oder was davon ausgeschlossen werden soll. Nach Anwendung eines Geltungsbereichs auf eine aktivierte Richtlinie werden Richtlinienereignisprüfungen auf den durch diesen Befehl definierten Geltungsbereich angewendet.

Benachrichtigungen werden für Dateizugriffsereignisse generiert, bei denen Übereinstimmungen in den Optionen „`include`“ gefunden werden. Benachrichtigungen werden nicht für Dateizugriffsereignisse generiert, bei denen Übereinstimmungen in den Optionen „`exclude`“ gefunden werden.

Die FPolicy Bereichskonfiguration definiert die folgenden Konfigurationsinformationen:

- SVM-Name
- Richtlinienname
- Die Freigaben, die in die Überwachung einbezogen oder von dieser ausgeschlossen werden
- Die Exportrichtlinien, die in die Überwachung einbezogen oder ausgeschlossen werden
- Die Volumes, die in die Überwachung einbezogen oder von dieser ausgeschlossen werden
- Die Dateierweiterungen, die in die Überwachung einbezogen oder von dieser ausgeschlossen werden
- Ob Dateierweiterungsprüfungen für Verzeichnisobjekte durchgeführt werden

> Für den Geltungsbereich einer Cluster FPolicy Richtlinie gelten besondere Bestimmungen. Die Cluster FPolicy Richtlinie ist eine Richtlinie, die der Clusteradministrator für die Admin SVM erstellt. Wenn der Clusteradministrator auch den Geltungsbereich für diese Cluster FPolicy Richtlinie festlegt, kann der SVM-Administrator keinen Geltungsbereich für dieselbe Richtlinie erstellen. Legt der Clusteradministrator jedoch keinen Geltungsbereich für die Cluster FPolicy Richtlinie fest, kann jeder SVM-Administrator den Geltungsbereich für diese Cluster Richtlinie erstellen. Hat der SVM-Administrator bereits einen Geltungsbereich für diese Cluster FPolicy Richtlinie erstellt, kann der Clusteradministrator anschließend keinen weiteren Geltungsbereich für dieselbe Cluster Richtlinie erstellen. Dies liegt daran, dass der Clusteradministrator den Geltungsbereich für dieselbe Cluster Richtlinie nicht überschreiben kann.

Was die Vorrangregeln des Geltungsbereichs sind

Für Bereichskonfigurationen gelten folgende Vorrangregeln:

- Wenn ein Share im `-shares-to-include` Parameter enthalten ist und das übergeordnete Volume des Shares im `-volumes-to-exclude` Parameter enthalten ist, hat `-volumes-to-exclude` Vorrang vor

`-shares-to-include`.

- Wenn eine Exportrichtlinie im `-export-policies-to-include` Parameter enthalten ist und das übergeordnete Volume der Exportrichtlinie im `-volumes-to-exclude` Parameter enthalten ist, `-volumes-to-exclude` hat Vorrang vor `-export-policies-to-include`.
- Ein Administrator kann sowohl `-file-extensions-to-include` als auch `-file-extensions-to-exclude` Listen angeben.

  Der `-file-extensions-to-exclude`Parameter wird geprüft, bevor der `-file-extensions-to-include`Parameter geprüft wird.

Was die FPolicy Bereichskonfiguration enthält

Die folgende Liste der verfügbaren FPolicy Bereichskonfigurationsparameter kann bei der Planung Ihrer Konfiguration unterstützen:

> Bei der Konfiguration der einzuschließenden oder auszuschließenden Freigaben, Exportrichtlinien, Volumes und Dateierweiterungen können die Parameter für Ein- und Ausschluss Metazeichen wie “?” and “*” enthalten. Die Verwendung regulärer Ausdrücke wird nicht unterstützt.

Art der Information	Option
SVM Gibt den SVM-Namen an, auf dem ein FPolicy-Bereich erstellt werden soll. Jede FPolicy Konfiguration ist innerhalb einer einzelnen SVM definiert. Die externe Engine, das Richtlinienereignis, der Richtlinienbereich und die Richtlinie, die zusammen eine FPolicy Richtlinienkonfiguration bilden, müssen alle derselben SVM zugeordnet sein.	`-vserver vserver_name`
Richtlinienname Gibt den Namen der FPolicy Richtlinie an, der der Bereich zugeordnet werden soll. Die FPolicy Richtlinie muss bereits vorhanden sein.	`-policy-name policy_name`
Einzuschließende Shares Gibt eine durch Kommas getrennte Liste von Shares an, die für die FPolicy Richtlinie, auf die der Geltungsbereich angewendet wird, überwacht werden.	`-shares-to-include share_name, ...`
Auszuschließende Shares Gibt eine durch Kommas getrennte Liste von Shares an, die von der Überwachung für die FPolicy Richtlinie, auf die der Geltungsbereich angewendet wird, ausgeschlossen werden.	`-shares-to-exclude share_name, ...`
Einzuschließende Volumes Gibt eine durch Kommas getrennte Liste von Volumes an, die für die FPolicy Richtlinie, auf die der Geltungsbereich angewendet wird, überwacht werden.	`-volumes-to-include volume_name, ...`
Auszuschließende Volumes Gibt eine durch Kommas getrennte Liste von Volumes an, die von der Überwachung für die FPolicy Richtlinie, auf die der Geltungsbereich angewendet wird, ausgeschlossen werden.	`-volumes-to-exclude volume_name, ...`

Zu berücksichtigende Exportrichtlinien Gibt eine durch Kommas getrennte Liste von Exportrichtlinien an, die für die FPolicy Richtlinie überwacht werden, auf die der Geltungsbereich angewendet wird.	`-export-policies-to -include export_policy_name, ...`
Auszuschließende Exportrichtlinien Gibt eine durch Kommas getrennte Liste von Exportrichtlinien an, die von der Überwachung für die FPolicy Richtlinie, auf die der Geltungsbereich angewendet wird, ausgeschlossen werden.	`-export-policies-to -exclude export_policy_name, ...`
Einzuschließende Dateierweiterungen Gibt eine durch Kommas getrennte Liste von Dateierweiterungen an, die für die FPolicy Richtlinie, auf die der Bereich angewendet wird, überwacht werden.	`-file-extensions-to -include file_extensions, ...`
Auszuschließende Dateierweiterung Gibt eine durch Kommas getrennte Liste von Dateierweiterungen an, die von der Überwachung für die FPolicy Richtlinie, auf die der Bereich angewendet wird, ausgeschlossen werden.	`-file-extensions-to -exclude file_extensions, ...`
Ist die Dateierweiterungsprüfung für Verzeichnisse aktiviert? Legt fest, ob die Überprüfung der Dateinamenerweiterung auch für Verzeichnisobjekte gilt. Wenn dieser Parameter auf `true` gesetzt ist, werden die Verzeichnisobjekte denselben Erweiterungsprüfungen unterzogen wie reguläre Dateien. Wenn dieser Parameter auf `false` gesetzt ist, werden die Verzeichnisnamen nicht auf Erweiterungen geprüft und Benachrichtigungen werden auch für Verzeichnisse gesendet, selbst wenn deren Namensendungen nicht übereinstimmen. Wenn die FPolicy Richtlinie, der der Bereich zugewiesen ist, für die Verwendung der nativen Engine konfiguriert ist, muss dieser Parameter auf `true` gesetzt werden.	`-is-file-extension -check-on-directories -enabled {true`
`false`	}

ONTAP FPolicy Arbeitsblätter zum Geltungsbereich

Sie können dieses Arbeitsblatt verwenden, um die Werte zu erfassen, die Sie während des FPolicy Scope-Konfigurationsprozesses benötigen. Wenn ein Parameterwert erforderlich ist, muss vor der Konfiguration des FPolicy Scope festgelegt werden, welcher Wert für diese Parameter verwendet wird.

Es sollte festgehalten werden, ob jede Parametereinstellung in die FPolicy Bereichskonfiguration aufgenommen werden soll, und anschließend der Wert für die Parameter, die aufgenommen werden sollen, dokumentiert werden.

Art der Information	Erforderlich	Enthalten	Ihre Werte
Name der Storage Virtual Machine (SVM)	Ja	Ja	
Richtlinienname	Ja	Ja	

Freigaben, die einbezogen werden sollen	Nein		
Auszuschließende Shares	Nein		
Einzuschließende Volumes	Nein		
Auszuschließende Volumes	Nein		
Einzuschließende Exportrichtlinien	Nein		
Zu ausschließende Exportrichtlinien	Nein		
Zu berücksichtigende Dateierweiterungen	Nein		
Auszuschließende Dateierweiterung	Nein		
Ist die Dateierweiterungsprüfung für Verzeichnisse aktiviert?	Nein		

Die FPolicy Konfiguration erstellen

ONTAP FPolicy externe Engines erstellen

Sie müssen eine externe Engine erstellen, um mit der Erstellung einer FPolicy-Konfiguration zu beginnen. Die externe Engine definiert, wie FPolicy Verbindungen zu externen FPolicy-Servern herstellt und verwaltet. Wenn Ihre Konfiguration die interne ONTAP Engine (die native externe Engine) für einfaches Dateiblockieren verwendet, ist keine separate FPolicy externe Engine zu konfigurieren und dieser Schritt ist nicht erforderlich.

Bevor Sie beginnen

Das "externe Engine" Arbeitsblatt sollte ausgefüllt werden.

Über diese Aufgabe

Wenn die externe Engine in einer MetroCluster Konfiguration verwendet wird, sollten die IP-Adressen der FPolicy-Server am Quellstandort als primäre Server angegeben werden. Die IP-Adressen der FPolicy-Server am Zielstandort sollten als sekundäre Server angegeben werden.

Schritte

1. Die externe FPolicy Engine wird mit dem `vserver fpolicy policy external-engine create` Befehl erstellt.

   Der folgende Befehl erstellt eine externe Engine auf der Storage Virtual Machine (SVM) vs1.example.com. Für die externe Kommunikation mit dem FPolicy Server ist keine Authentifizierung erforderlich.

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

2. Die Konfiguration der externen FPolicy Engine kann mithilfe des `vserver fpolicy policy external-engine show` Befehls überprüft werden.

   Der folgende Befehl zeigt Informationen über alle auf SVM vs1.example.com konfigurierten externen Engines an:

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

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

Der folgende Befehl zeigt detaillierte Informationen über die externe Engine mit dem Namen “engine1” auf SVM vs1.example.com an:

```
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: -
```

ONTAP FPolicy-Ereignisse erstellen

Im Rahmen der Erstellung einer FPolicy Richtlinienkonfiguration ist ein FPolicy Ereignis zu erstellen. Das Ereignis wird mit der FPolicy Richtlinie verknüpft, wenn diese erstellt wird. Ein Ereignis legt fest, welches Protokoll überwacht wird und welche Dateizugriffsereignisse überwacht und gefiltert werden.

Bevor Sie beginnen

Das FPolicy-Ereignis sollte abgeschlossen werden "Arbeitsblatt".

Das FPolicy Ereignis erstellen

1. Das FPolicy Ereignis wird mit dem `vserver fpolicy policy event create` Befehl erstellt.

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

2. Die FPolicy Ereigniskonfiguration kann mit dem `vserver fpolicy policy event show` Befehl überprüft werden.

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

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

Die FPolicy Access Denied-Ereignisse erstellen

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen über fehlgeschlagene Dateivorgänge aufgrund fehlender Berechtigungen erhalten. Diese Benachrichtigungen sind wertvoll für Sicherheit, Ransomware-Schutz und Governance.

1. Das FPolicy Ereignis wird mit dem `vserver fpolicy policy event create` Befehl erstellt.

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

ONTAP FPolicy persistente Speicher erstellen

Persistente Speicher können die Client-E/A-Verarbeitung von der FPolicy-Benachrichtigungsverarbeitung entkoppeln, um die Client-Latenz zu reduzieren. Ab ONTAP 9.14.1 ermöglicht FPolicy die Einrichtung von "persistente Speicher" zum Erfassen von Dateizugriffsereignissen für asynchrone, nicht obligatorische Richtlinien in der SVM. Synchrone (obligatorische oder nicht obligatorische) und asynchron obligatorische Konfigurationen werden nicht unterstützt.

Ab ONTAP 9.15.1 ist die Konfiguration des persistenten Speichers mit FPolicy vereinfacht. Der `persistent-store create` Befehl automatisiert die Volume-Erstellung für die SVM und konfiguriert das Volume für den persistenten Store.

Es gibt zwei Möglichkeiten, einen persistenten Speicher zu erstellen, abhängig von der ONTAP-Version:

- ONTAP 9.15.1 oder höher: Beim Erstellen des persistenten Speichers erstellt und konfiguriert ONTAP automatisch gleichzeitig dessen Volume. Dies vereinfacht die FPolicy Persistent Store Konfiguration und implementiert alle Best Practices.
- ONTAP 9.14.1: Manuelles Erstellen und Konfigurieren eines Volumes und anschließendes Erstellen eines persistenten Speichers für das neu erstellte Volume.

Auf jeder SVM kann nur ein persistenter Speicher eingerichtet werden. Dieser einzelne persistente Speicher muss für alle FPolicy Konfigurationen auf dieser SVM verwendet werden, selbst wenn die Richtlinien von verschiedenen Partnern stammen.

Persistenten Speicher erstellen (ONTAP 9.15.1 oder höher)

Ab ONTAP 9.15.1 kann der `fpolicy persistent-store create` Befehl verwendet werden, um den FPolicy persistenten Store mit Inline-Volume-Erstellung und -Konfiguration zu erstellen. ONTAP blockiert automatisch den Volume-Zugriff über externe Benutzerprotokolle (CIFS/NFS).

Bevor Sie beginnen

- Die SVM, in der der persistente Speicher erstellt werden soll, muss mindestens ein Aggregat haben.
- Sie sollten Zugriff auf die für die SVM verfügbaren Aggregate und ausreichende Berechtigungen zum Erstellen von Volumes haben.

Schritte

1. Der persistente Speicher wird erstellt, wobei das Volume automatisch erstellt und konfiguriert wird:

   ```
   vserver fpolicy persistent-store create -vserver <vserver> -persistent-store
   <name> -volume <volume_name> -size <size> -autosize-mode
   <off|grow|grow_shrink>
   ```

   - Der `vserver` Parameter ist der Name der SVM.
   - Der `persistent-store` Parameter ist der Name des persistenten Speichers.
   - Der `volume` Parameter ist der Name des persistenten Speichervolumes.

     Wenn Sie ein vorhandenes, leeres Volume verwenden möchten, verwenden Sie den `volume show` Befehl, um es zu finden und im Volume-Parameter anzugeben.

   - Der `size`Parameter basiert auf der Zeitdauer, für die die Ereignisse gespeichert werden sollen, die nicht an den externen Server (Partneranwendung) übermittelt werden.

     Wenn beispielsweise Ereignisse der letzten 30 Minuten in einem Cluster mit einer Kapazität von 30.000 Benachrichtigungen pro Sekunde erhalten bleiben sollen:

     Erforderliche Volume-Größe = 30000 x 30 x 60 x 0,6 KB (durchschnittliche Größe eines Benachrichtigungsdatensatzes) = 32400000 KB = ~32 GB

     Um die ungefähre Benachrichtigungsrate zu ermitteln, können Sie entweder Ihre FPolicy Partneranwendung kontaktieren oder den FPolicy Zähler verwenden `requests_dispatched_rate`.

     Wenn Sie ein vorhandenes Volume verwenden, ist der Größenparameter optional. Wenn Sie einen Wert für den Größenparameter angeben, wird das Volume mit der von Ihnen angegebenen Größe geändert.

   - Der `autosize-mode`Parameter gibt den Modus für die automatische Größenanpassung des Volumes an. Die unterstützten Modi für die automatische Größenanpassung sind:
     - Aus - Das Volumen wächst oder schrumpft nicht in der Größe in Abhängigkeit vom genutzten Speicherplatz.
     - wachsen - Das Volumen wird automatisch vergrößert, wenn der belegte Speicherplatz im Volumen über dem Wachstumsschwellenwert liegt.
     - grow_shrink - Das Volumen vergrößert oder verkleinert sich in Abhängigkeit vom genutzten Speicherplatz.

2. Die FPolicy Richtlinie wird erstellt und der Name des persistenten Speichers zu dieser Richtlinie hinzugefügt. Weitere Informationen finden sich unter "Die FPolicy Richtlinie erstellen".

Erstellen eines persistenten Speichers (ONTAP 9.14.1)

Sie können ein Volume erstellen und anschließend einen persistenten Speicher einrichten, der dieses Volume nutzt. Anschließend kann der Zugriff externer Benutzerprotokolle (CIFS/NFS) auf das neu erstellte Volume gesperrt werden.

Schritte

1. Ein leeres Volume auf der SVM erstellen, das für den persistenten Speicher bereitgestellt werden kann:

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

   Es wird erwartet, dass ein Administratorbenutzer mit ausreichenden RBAC-Berechtigungen (zum Erstellen eines Volumes) ein Volume (mittels des CLI-Befehls volume oder der REST-API) in der gewünschten Größe erstellt und den Namen dieses Volumes als `-volume` im CLI-Befehl persistent store create oder in der REST-API angibt.

   - Der `vserver` Parameter ist der Name der SVM.
   - Der `volume` Parameter ist der Name des persistenten Speichervolumes.
   - Der `state`Parameter sollte auf „online“ eingestellt werden, damit das Volume verfügbar ist.
   - Der `policy` Parameter wird auf die FPolicy Service-Richtlinie gesetzt, sofern bereits eine konfiguriert ist. Falls nicht, kann die `volume modify` Richtlinie später mit dem Befehl hinzugefügt werden.
   - Der `unix-permissions` Parameter ist optional.
   - Der `size`Parameter basiert auf der Zeitdauer, für die die Ereignisse gespeichert werden sollen, die nicht an den externen Server (Partneranwendung) übermittelt werden.

     Wenn beispielsweise Ereignisse der letzten 30 Minuten in einem Cluster mit einer Kapazität von 30.000 Benachrichtigungen pro Sekunde erhalten bleiben sollen:

     Erforderliche Volume-Größe = 30000 x 30 x 60 x 0,6 KB (durchschnittliche Größe eines Benachrichtigungsdatensatzes) = 32400000 KB = ~32 GB

   Um die ungefähre Benachrichtigungsrate zu ermitteln, können Sie entweder Ihre FPolicy Partneranwendung kontaktieren oder den FPolicy Zähler verwenden `requests_dispatched_rate`.

   - Der Aggregatparameter wird für FlexVol Volumes benötigt, ansonsten ist er nicht erforderlich.
   - Der `snapshot-policy` Parameter muss auf „none“ gesetzt werden. Dadurch ist sichergestellt, dass keine versehentliche Wiederherstellung des Snapshots erfolgt, die zum Verlust aktueller Ereignisse führen und eine mögliche doppelte Ereignisverarbeitung verhindern könnte.

     Wenn ein vorhandenes, leeres Volume verwendet werden soll, kann der `volume show` Befehl genutzt werden, um es zu finden, und der `volume modify` Befehl, um die erforderlichen Änderungen vorzunehmen. Es ist sicherzustellen, dass Richtlinie, Größe und `snapshot-policy` Parameter für den persistenten Speicher korrekt eingestellt sind.

2. Den persistenten Speicher erstellen:

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

- Der `vserver` Parameter ist der Name der SVM.
- Der `persistent-store` Parameter ist der Name des persistenten Speichers.
- Der `volume` Parameter ist der Name des persistenten Speichervolumes.

3. Die FPolicy Richtlinie wird erstellt und der Name des persistenten Speichers zu dieser Richtlinie hinzugefügt. Weitere Informationen finden sich unter "Die FPolicy Richtlinie erstellen".

ONTAP FPolicy-Richtlinien erstellen

Beim Erstellen der FPolicy Richtlinie wird eine externe Engine und ein oder mehrere Ereignisse mit der Richtlinie verknüpft. Die Richtlinie gibt außerdem an, ob eine obligatorische Überprüfung erforderlich ist, ob die FPolicy Server privilegierten Zugriff auf Daten auf der Storage Virtual Machine (SVM) haben und ob Passthrough-Read für Offline-Dateien aktiviert ist.

Bevor Sie beginnen

- Das FPolicy Richtlinienarbeitsblatt sollte ausgefüllt werden.
- Wenn die Richtlinie so konfiguriert wird, dass FPolicy Server verwendet werden, muss die externe Engine vorhanden sein.
- Mindestens ein FPolicy-Ereignis, das mit der FPolicy-Richtlinie verknüpft werden soll, muss vorhanden sein.
- Wenn Sie den privilegierten Datenzugriff konfigurieren möchten, muss auf der SVM ein SMB-Server vorhanden sein.
- Um einen persistenten Speicher für eine Richtlinie zu konfigurieren, muss der Engine-Typ **async** sein und die Richtlinie muss **non-mandatory** sein.

  Weitere Informationen finden sich unter "Persistente Speicher erstellen".

- Ab ONTAP 9.20.1 unterstützen FPolicy-Richtlinien S3-Ereignisse, allerdings mit einigen Einschränkungen. FPolicy-Richtlinien mit S3-Ereignissen können Folgendes nicht verwenden:
  - Externe Engine mit aktivierter Ausfallsicherheit
  - Externe Engine mit SSL (Server-Authentifizierung oder gegenseitige Authentifizierung)
  - Externe Engine mit XML-Format
  - Pflichtmodus (-is-mandatory true)
  - Nativ-Engine
  - Persistenter Speicher
  - Privilegierter Zugriff / Passthrough-Lesezugriff
  - Synchrone externe Engine

Schritte

1. Die FPolicy Richtlinie erstellen:

```
vserver fpolicy policy create -vserver <vserver_name> -policy-name
```

`<policy_name> -engine <engine_name> -events <event_name>[,event_name2,…] [-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}]`

- Sie können der FPolicy Policy ein oder mehrere durch Kommas getrennte Ereignisse hinzufügen.
- Standardmäßig ist die obligatorische Überprüfung aktiviert.
- Wenn privilegierter Zugriff durch Setzen des `-allow-privileged-access` Parameters auf `yes` erlaubt werden soll, muss auch ein privilegierter Benutzername für den privilegierten Zugriff konfiguriert werden.
- Wenn passthrough-read durch Setzen des `-is-passthrough-read-enabled` Parameters auf `true` konfiguriert werden soll, muss auch der privilegierte Datenzugriff konfiguriert werden.

  Der folgende Befehl erstellt eine Richtlinie mit dem Namen `policy1`, der das Ereignis mit dem Namen `event1` und die externe Engine mit dem Namen `engine1` zugeordnet sind. Diese Richtlinie verwendet Standardwerte in der Richtlinienkonfiguration: `vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

  Der folgende Befehl erstellt eine Richtlinie mit dem Namen `policy2`, der das Ereignis mit dem Namen `event2` und die externe Engine mit dem Namen `engine2` zugeordnet sind. Diese Richtlinie ist so konfiguriert, dass privilegierter Zugriff mit dem angegebenen Benutzernamen verwendet wird. Passthrough-Read ist aktiviert:

  ```
  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
  ```

  Der folgende Befehl erstellt eine Richtlinie mit dem Namen `native1`, der das Ereignis `event3` zugeordnet ist. Diese Richtlinie verwendet die native Engine und verwendet Standardwerte in der Richtlinienkonfiguration:

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

2. Die FPolicy Richtlinienkonfiguration kann mit dem `vserver fpolicy policy show` Befehl überprüft werden.

   Der folgende Befehl zeigt Informationen zu den drei konfigurierten FPolicy Richtlinien an, einschließlich der folgenden Informationen:

   - Die mit der Richtlinie verbundene SVM
   - Die externe Engine, die mit der Richtlinie verknüpft ist
   - Die mit der Richtlinie verbundenen Ereignisse
   - Ob eine obligatorische Überprüfung erforderlich ist
   - Ob ein privilegierter Zugriff erforderlich ist `vserver fpolicy policy show`

```
   Vserver       Policy     Events    Engine    Is Mandatory  Privileged
                 Name                                       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
```

ONTAP FPolicy-Bereiche erstellen

Nach dem Erstellen der FPolicy Richtlinie ist ein FPolicy Bereich zu erstellen. Beim Erstellen des Bereichs wird dieser mit einer FPolicy Richtlinie verknüpft. Ein Bereich definiert die Grenzen, auf die die FPolicy Richtlinie angewendet wird. Bereiche können Dateien basierend auf Freigaben, Exportrichtlinien, Volumes und Dateierweiterungen ein- oder ausschließen.

Ab ONTAP 9.20.1 unterstützt FPolicy die S3-Überwachung. Der Geltungsbereich von S3 FPolicy kann mithilfe dieser Parameter auf bestimmte NAS-Buckets beschränkt werden:

- `-nas-buckets-to-include`
- `-nas-buckets-to-exclude`

Bevor Sie beginnen

Das FPolicy Scope-Arbeitsblatt muss ausgefüllt werden. Die FPolicy Richtlinie muss mit einer zugehörigen externen Engine vorhanden sein (falls die Richtlinie für die Verwendung externer FPolicy Server konfiguriert ist) und mindestens ein zugehöriges FPolicy Ereignis aufweisen.

Schritte

1. Der FPolicy-Bereich wird mithilfe des `vserver fpolicy policy scope create` Befehls erstellt.

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

2. Die FPolicy Bereichskonfiguration kann mit dem `vserver fpolicy policy scope show` Befehl überprüft werden.

   ```
   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: -
   ```

ONTAP FPolicy Richtlinien aktivieren

Nachdem die Konfiguration einer FPolicy Richtlinie abgeschlossen ist, wird die FPolicy Richtlinie aktiviert. Durch das Aktivieren der Richtlinie werden deren Priorität festgelegt und die Überwachung des Dateizugriffs für die Richtlinie gestartet.

Bevor Sie beginnen

Die FPolicy Richtlinie muss mit einer zugehörigen externen Engine vorhanden sein (falls die Richtlinie für die Verwendung externer FPolicy Server konfiguriert ist) und mindestens ein zugehöriges FPolicy Ereignis aufweisen. Der Gültigkeitsbereich der FPolicy Richtlinie muss vorhanden sein und der FPolicy Richtlinie zugewiesen werden.

Über diese Aufgabe

Die Priorität wird verwendet, wenn mehrere Richtlinien auf der Storage Virtual Machine (SVM) aktiviert sind und mehr als eine Richtlinie dasselbe Dateizugriff-Ereignis abonniert hat. Richtlinien, die die native Engine-Konfiguration verwenden, haben eine höhere Priorität als Richtlinien für jede andere Engine, unabhängig von der ihnen bei der Aktivierung der Richtlinie zugewiesenen Sequenznummer.

Auf der Admin-SVM kann keine Richtlinie aktiviert werden.

Schritte

1. Die FPolicy Richtlinie wird mit dem `vserver fpolicy enable`Konfigurationsbefehl aktiviert.

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

2. Es kann mit dem `vserver fpolicy show` Befehl überprüft werden, ob die FPolicy Richtlinie aktiviert ist.

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

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

FPolicy Konfigurationen verwalten

FPolicy Konfigurationen anpassen

Befehle zum Ändern von FPolicy Konfigurationen in ONTAP

Sie können FPolicy Konfigurationen anpassen, indem Sie die Elemente ändern, aus denen die Konfiguration besteht. Sie können externe Engines, FPolicy Events, FPolicy Scopes, FPolicy Persistent Stores und FPolicy Policies ändern. FPolicy Policies können außerdem aktiviert oder deaktiviert werden. Wenn die FPolicy Policy deaktiviert wird, wird die Dateiüberwachung für diese Policy eingestellt.

Sie sollten eine FPolicy Richtlinie deaktivieren, bevor deren Konfiguration geändert wird.

Wenn Sie Änderungen vornehmen möchten…	Verwenden Sie diesen Befehl…
Externe Engines	`vserver fpolicy policy external-engine modify`
Veranstaltungen	`vserver fpolicy policy event modify`
Bereiche	`vserver fpolicy policy scope modify`
Persistenter Speicher	`vserver fpolicy persistent-store modify`
Richtlinien	`vserver fpolicy policy modify`

Weitere Informationen zu `vserver fpolicy policy` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP FPolicy Richtlinien aktivieren oder deaktivieren

FPolicy-Richtlinien können nach Abschluss der Konfiguration aktiviert werden. Durch das Aktivieren der Richtlinie werden deren Priorität festgelegt und die Überwachung des Dateizugriffs für die Richtlinie gestartet. FPolicy-Richtlinien können deaktiviert werden, wenn die Dateizugriffsüberwachung für diese Richtlinie beendet werden soll.

Bevor Sie beginnen

Bevor FPolicy Richtlinien aktiviert werden, muss die FPolicy Konfiguration abgeschlossen sein.

Über diese Aufgabe

- Die Priorität wird verwendet, wenn mehrere Richtlinien auf der Storage Virtual Machine (SVM) aktiviert sind und mehr als eine Richtlinie dasselbe Dateizugriff-Ereignis abonniert hat.
- Richtlinien, die die native Engine-Konfiguration verwenden, haben eine höhere Priorität als Richtlinien für jede andere Engine, unabhängig von der ihnen bei der Aktivierung der Richtlinie zugewiesenen Sequenznummer.
- Wenn die Priorität einer FPolicy Richtlinie geändert werden soll, ist es erforderlich, die Richtlinie zu deaktivieren und anschließend mit der neuen Sequenznummer wieder zu aktivieren.

Schritt

1. Die entsprechende Maßnahme ausführen:

Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
Aktivieren einer FPolicy Richtlinie	`vserver fpolicy enable -vserver <svm_name> -policy -name <policy_name> [-sequence-number <integer>]`
Eine FPolicy Richtlinie deaktivieren	`vserver fpolicy disable -vserver <svm_name> -policy-name <policy_name>`

Informationen zu FPolicy Konfigurationen

Informationen zu ONTAP FPolicy show-Befehlen

Beim Anzeigen von Informationen zur FPolicy Konfiguration ist es hilfreich zu verstehen, wie die `show` Befehle funktionieren.

Ein `show` Befehl ohne zusätzliche Parameter zeigt Informationen in zusammengefasster Form an. Zusätzlich verfügt jeder `show` Befehl über dieselben zwei sich gegenseitig ausschließenden optionalen Parameter, `-instance` und `-fields`.

Wenn Sie den `-instance` Parameter mit einem `show` Befehl verwenden, zeigt die Befehlsausgabe detaillierte Informationen in Listenform an. In einigen Fällen kann die detaillierte Ausgabe sehr umfangreich sein und mehr Informationen enthalten, als benötigt werden. Mit dem `-fields fieldname[,fieldname…]` Parameter lässt sich die Ausgabe anpassen, sodass nur Informationen zu den von Ihnen angegebenen Feldern angezeigt werden. Welche Felder angegeben werden können, lässt sich durch die Eingabe von `?` nach dem `-fields` Parameter ermitteln.

Die Ausgabe eines `show` Kommandos mit dem `-fields` Parameter kann weitere relevante und notwendige Felder anzeigen, die mit den angeforderten Feldern in Zusammenhang stehen.

Jeder `show` Befehl verfügt über einen oder mehrere optionale Parameter, die die Ausgabe filtern und es ermöglichen, den Umfang der angezeigten Informationen einzugrenzen. Es kann festgestellt werden, welche optionalen Parameter für einen Befehl verfügbar sind, indem `?` nach dem `show` Befehl eingegeben wird.

Der `show` Befehl unterstützt UNIX-typische Muster und Platzhalter, um mehrere Werte in Befehlsparameterargumenten abzugleichen. Beispielsweise können der Platzhalteroperator (*), der NOT-Operator (!), der OR-Operator (|), der Bereichsoperator (integer…integer), der Kleiner-als-Operator (<), the greater-than operator (>), der Kleiner-gleich-Operator (<=), and the greater-than or equal to operator (>=) beim Angeben von Werten verwendet werden.

Weitere Informationen zur Verwendung von UNIX-Mustern und Wildcards sind unter Verwendung der ONTAP Befehlszeilenschnittstelle zu finden.

Befehle zum Anzeigen von Informationen über FPolicy Konfigurationen in ONTAP

Die `fpolicy show` Befehle werden verwendet, um Informationen zur FPolicy Konfiguration anzuzeigen, einschließlich Informationen zu FPolicy External Engines, Ereignissen, Geltungsbereichen und Richtlinien.

Wenn Sie Informationen über FPolicy anzeigen möchten…	Verwenden Sie diesen Befehl…
Externe Engines	`vserver fpolicy policy external-engine show`
Veranstaltungen	`vserver fpolicy policy event show`
Bereiche	`vserver fpolicy policy scope show`
Richtlinien	`vserver fpolicy policy show`

Weitere Informationen zu `vserver fpolicy policy` finden sich in der "ONTAP-Befehlsreferenz".

Informationen zum Status der ONTAP FPolicy Richtlinie

Sie können Informationen über den Status von FPolicy Richtlinien anzeigen, um festzustellen, ob eine Richtlinie aktiviert ist, welche externe Engine für deren Verwendung konfiguriert ist, welche Sequenznummer die Richtlinie hat und welcher Storage Virtual Machine (SVM) die FPolicy Richtlinie zugeordnet ist.

Über diese Aufgabe

Wenn Sie keine Parameter angeben, zeigt der Befehl folgende Informationen an:

- SVM-Name
- Richtlinienname
- Policy-Sequenznummer
- Richtlinienstatus

Zusätzlich zur Anzeige von Informationen über den Richtlinienstatus für auf dem Cluster oder eine bestimmte SVM konfigurierte FPolicy Richtlinien können Befehlsparameter verwendet werden, um die Ausgabe des Befehls nach anderen Kriterien zu filtern.

Sie können den `-instance` Parameter angeben, um detaillierte Informationen zu den aufgelisteten Richtlinien anzuzeigen. Alternativ kann der `-fields` Parameter verwendet werden, um nur die angegebenen Felder in der Befehlsausgabe anzuzeigen, oder `-fields ?` um zu bestimmen, welche Felder verwendet werden können.

Schritt

1. Gefilterte Informationen zum FPolicy Richtlinienstatus werden mit dem entsprechenden Befehl angezeigt:

Wenn Statusinformationen zu Richtlinien angezeigt werden sollen…	Geben Sie den Befehl ein…
Auf dem Cluster	`vserver fpolicy show`
Die den angegebenen Status haben	`vserver fpolicy show -status {on
off}`	Auf einer bestimmten SVM
`vserver fpolicy show -vserver vserver_name`	Mit dem angegebenen Richtliniennamen
`vserver fpolicy show -policy-name policy_name`	Die die angegebene externe Engine verwenden

Beispiel

Das folgende Beispiel zeigt die Informationen zu den FPolicy Richtlinien im Cluster an:

```
cluster1::> vserver fpolicy show
                                      Sequence
Vserver             Policy Name         Number  Status      Engine
------------------- ------------------- --------  ---------   ---------
FPolicy             cserver_policy      -         off         eng1
vs1.example.com     v1p1                -         off         eng2
vs1.example.com     v1p2                -         off         native
vs1.example.com     v1p3                -         off         native
vs1.example.com     cserver_policy      -         off         eng1
vs2.example.com     v1p1                3         on          native
vs2.example.com     v1p2                1         on          eng3
```

```
vs2.example.com     cserver_policy      2          on          eng1
```

Informationen zu aktivierten ONTAP FPolicy Richtlinien

Sie können Informationen über aktivierte FPolicy Richtlinien anzeigen, um festzustellen, welche FPolicy External Engine verwendet wird, welche Priorität die Richtlinie hat und welcher Storage Virtual Machine (SVM) die FPolicy Richtlinie zugeordnet ist.

Über diese Aufgabe

Wenn Sie keine Parameter angeben, zeigt der Befehl folgende Informationen an:

- SVM-Name
- Richtlinienname
- Richtlinienpriorität

Mit Befehlsparametern lässt sich die Ausgabe des Befehls nach bestimmten Kriterien filtern.

Schritt

1. Informationen zu aktivierten FPolicy Richtlinien werden mithilfe des entsprechenden Befehls angezeigt:

Wenn Informationen über aktivierte Richtlinien angezeigt werden sollen…	Geben Sie den Befehl ein…
Auf dem Cluster	`vserver fpolicy show-enabled`
Auf einer bestimmten SVM	`vserver fpolicy show-enabled -vserver vserver_name`
Mit dem angegebenen Richtliniennamen	`vserver fpolicy show-enabled -policy-name policy_name`
Mit der angegebenen Sequenznummer	`vserver fpolicy show-enabled -priority integer`

Beispiel

Das folgende Beispiel zeigt die Informationen zu den aktivierten FPolicy Richtlinien im Cluster:

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

FPolicy Serververbindungen verwalten

Verbindung zu externen FPolicy Servern in ONTAP

Um die Dateiverarbeitung zu aktivieren, kann es erforderlich sein, manuell eine Verbindung zu einem externen FPolicy Server herzustellen, falls die Verbindung zuvor getrennt wurde. Eine Verbindung wird getrennt, nachdem die Server-Zeitüberschreitung erreicht wurde oder aufgrund eines Fehlers. Alternativ kann der Administrator eine Verbindung auch manuell beenden.

Über diese Aufgabe

Tritt ein schwerwiegender Fehler auf, kann die Verbindung zum FPolicy Server unterbrochen werden. Nachdem das Problem, das den schwerwiegenden Fehler verursacht hat, behoben wurde, ist eine manuelle Wiederherstellung der Verbindung zum FPolicy Server erforderlich.

Schritte

1. Mit dem `vserver fpolicy engine-connect` Befehl wird eine Verbindung zum externen FPolicy Server hergestellt.

   Weitere Informationen zu `vserver fpolicy engine-connect` finden sich in der "ONTAP-Befehlsreferenz".

2. Es kann mit dem `vserver fpolicy show-engine` Befehl überprüft werden, ob der externe FPolicy Server verbunden ist.

   Weitere Informationen zu `vserver fpolicy show-engine` finden sich in der "ONTAP-Befehlsreferenz".

Verbindung zu externen FPolicy Servern in ONTAP trennen

Möglicherweise muss die Verbindung zu einem externen FPolicy Server manuell getrennt werden. Dies kann sinnvoll sein, wenn der FPolicy Server Probleme bei der Verarbeitung von Benachrichtigungsanfragen hat oder wenn Wartungsarbeiten am FPolicy Server erforderlich sind.

Schritte

1. Die Verbindung zum externen FPolicy Server wird mit dem `vserver fpolicy engine-disconnect` Befehl getrennt.

   Weitere Informationen zu `vserver fpolicy engine-disconnect` finden sich in der "ONTAP-Befehlsreferenz".

2. Es kann mit dem `vserver fpolicy show-engine` Befehl überprüft werden, ob die Verbindung zum externen FPolicy Server getrennt ist.

   Weitere Informationen zu `vserver fpolicy show-engine` finden sich in der "ONTAP-Befehlsreferenz".

Verbindungen zu externen ONTAP FPolicy-Servern anzeigen

Sie können Statusinformationen zu Verbindungen zu externen FPolicy Servern (FPolicy Servern) für den Cluster oder eine bestimmte Storage Virtual Machine (SVM) anzeigen. Diese Informationen können dabei helfen zu bestimmen, welche FPolicy Server

verbunden sind.

Über diese Aufgabe

Wenn Sie keine Parameter angeben, zeigt der Befehl folgende Informationen an:

- SVM-Name
- Knotenname
- FPolicy Richtlinienname
- IP-Adresse des FPolicy Servers
- FPolicy Serverstatus
- FPolicy Servertyp

Zusätzlich zur Anzeige von Informationen über FPolicy-Verbindungen im Cluster oder einer bestimmten SVM lassen sich Befehlsparameter verwenden, um die Ausgabe des Befehls nach anderen Kriterien zu filtern.

Sie können den `-instance` Parameter angeben, um detaillierte Informationen zu den aufgelisteten Richtlinien anzuzeigen. Alternativ kann der `-fields` Parameter verwendet werden, um nur die angegebenen Felder in der Befehlsausgabe anzuzeigen. Sie können `?` nach dem `-fields` Parameter eingeben, um herauszufinden, welche Felder verwendet werden können.

Schritt

1. Gefilterte Informationen zum Verbindungsstatus zwischen dem Knoten und dem FPolicy Server werden mithilfe des entsprechenden Befehls angezeigt:

Wenn Verbindungsstatusinformationen zu FPolicy Servern angezeigt werden sollen…	Eingeben…
Die Sie angeben	`vserver fpolicy show-engine -server IP_address`
Für eine bestimmte SVM	`vserver fpolicy show-engine -vserver vserver_name`
Die mit einer bestimmten Richtlinie verknüpft sind	`vserver fpolicy show-engine -policy-name policy_name`
Mit dem von Ihnen angegebenen Serverstatus	`vserver fpolicy show-engine -server-status status` Der Serverstatus kann einer der folgenden sein: • `connected` • `disconnected` • `connecting` • `disconnecting`

Mit dem angegebenen Typ	`vserver fpolicy show-engine -server-type type` Der FPolicy Servertyp kann einer der folgenden sein: • `primary` • `secondary`
Die getrennt wurden mit dem angegebenen Grund	`vserver fpolicy show-engine -disconnect-reason text` Eine Verbindungsunterbrechung kann verschiedene Ursachen haben. Die folgenden Gründe für eine Verbindungsunterbrechung sind häufig: • `Disconnect command received from CLI.` • `Error encountered while parsing notification response from FPolicy server.` • `FPolicy Handshake failed.` • `SSL handshake failed.` • `TCP Connection to FPolicy server failed.` • `The screen response message received from the FPolicy server is not valid.`

Beispiel

Dieses Beispiel zeigt Informationen über externe Engine-Verbindungen zu FPolicy-Servern auf SVM vs1.example.com:

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                              Server-       Server-
Vserver         Policy    Node         Server        status        type
--------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1   node1        10.1.1.2      connected     primary
vs1.example.com policy1   node1        10.1.1.3      disconnected  primary
vs1.example.com policy1   node2        10.1.1.2      connected     primary
vs1.example.com policy1   node2        10.1.1.3      disconnected  primary
```

Dieses Beispiel zeigt nur Informationen über verbundene FPolicy Server an:

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver         policy-name server
---------- --------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
```

```
node2      vs1.example.com policy1     10.1.1.2
```

Status der ONTAP FPolicy Passthrough-Leseverbindung anzeigen

Sie können Informationen zum Status der Passthrough-Read-Verbindung zu externen FPolicy Servern (FPolicy Server) für den Cluster oder eine bestimmte Storage Virtual Machine (SVM) anzeigen. Diese Informationen können dabei helfen zu erkennen, welche FPolicy Server über Passthrough-Read-Datenverbindungen verfügen und bei welchen FPolicy Servern die Passthrough-Read-Verbindung getrennt ist.

Über diese Aufgabe

Wenn Sie keinen Parameter angeben, zeigt der Befehl die folgenden Informationen an:

- SVM-Name
- FPolicy Richtlinienname
- Knotenname
- IP-Adresse des FPolicy Servers
- FPolicy Passthrough-Read Verbindungsstatus

Zusätzlich zur Anzeige von Informationen über FPolicy-Verbindungen im Cluster oder einer bestimmten SVM lassen sich Befehlsparameter verwenden, um die Ausgabe des Befehls nach anderen Kriterien zu filtern.

Sie können den `-instance` Parameter angeben, um detaillierte Informationen zu den aufgelisteten Richtlinien anzuzeigen. Alternativ kann der `-fields` Parameter verwendet werden, um nur die angegebenen Felder in der Befehlsausgabe anzuzeigen. Sie können `?` nach dem `-fields` Parameter eingeben, um herauszufinden, welche Felder verwendet werden können.

Schritt

1. Gefilterte Informationen zum Verbindungsstatus zwischen dem Knoten und dem FPolicy Server werden mithilfe des entsprechenden Befehls angezeigt:

Wenn Verbindungsstatusinformationen über … angezeigt werden sollen	Geben Sie den Befehl ein…
FPolicy Passthrough-Read-Verbindungsstatus für den Cluster	`vserver fpolicy show-passthrough-read-connection`
FPolicy Passthrough-Read-Verbindungsstatus für eine bestimmte SVM	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`
FPolicy Passthrough-Read-Verbindungsstatus für eine bestimmte Richtlinie	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
Detaillierter Status der FPolicy Passthrough-Read-Verbindung für eine bestimmte Richtlinie	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`

FPolicy Passthrough-Read-Verbindungsstatus für den angegebenen Status	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status` Der Serverstatus kann einer der folgenden sein: • `connected` • `disconnected`

Beispiel

Der folgende Befehl zeigt Informationen über Passthrough-Leseverbindungen von allen FPolicy Servern im Cluster an:

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                          FPolicy           Server
Vserver          Policy Name   Node       Server            Status
---------------  ------------- ---------- ----------------
--------------
vs2.example.com  pol_cifs_2    FPolicy-01   2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
```

Der folgende Befehl zeigt detaillierte Informationen über Passthrough-Leseverbindungen von FPolicy-Servern an, die in der Richtlinie “pol_cifs_1” konfiguriert sind:

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                       Node: FPolicy-01
                                    Vserver: vs1.example.com
                                     Policy: pol_cifs_1
                                     Server: 1.1.1.1
               Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

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.