Planen der FPolicy-Konfiguration

ONTAP 9

NetApp
February 12, 2026

Inhalt

Planen der FPolicy-Konfiguration

Anforderungen, Überlegungen und Best Practices für die Konfiguration von ONTAP FPolicy

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

FPolicy-Funktionen werden entweder über die Befehlszeilenschnittstelle (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 Sie bestimmte Anforderungen kennen.

- Auf allen Nodes im Cluster muss eine Version von ONTAP ausgeführt werden, die FPolicy unterstützt.
- Wenn Sie nicht die native FPolicy Engine von ONTAP verwenden, müssen Sie externe FPolicy Server (FPolicy Server) installiert haben.
- Die FPolicy Server müssen auf einem Server installiert werden, auf den über die Daten-LIFs der SVM zugegriffen werden kann, wo FPolicy-Richtlinien aktiviert sind.

  Ab ONTAP 9.8 bietet ONTAP einen logischen Client-Service für ausgehende FPolicy-Verbindungen unter Hinzufügung des `data-fpolicy-client` Services. "Weitere Informationen zu LIFs und Service-Richtlinien".

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

    Der privilegierte Datenzugriff erfolgt über SMB-Verbindungen.

  - Für den Zugriff auf Dateien über den privilegierten Datenkanal müssen Benutzeranmeldeinformationen konfiguriert werden.
  - Der FPolicy-Server muss unter den in der FPolicy-Konfiguration konfigurierten Anmeldeinformationen ausgeführt werden.
  - Alle Daten-LIFs, die zur Kommunikation mit den FPolicy Servern verwendet werden, müssen so konfiguriert werden `cifs`, dass sie eines der zulässigen Protokolle besitzen.

    Dies schließt die LIFs ein, die für Passthrough-Read-Verbindungen verwendet werden.

Best Practices und Empfehlungen beim Einrichten von FPolicy

Wenn Sie FPolicy auf Storage Virtual Machines (SVMs) einrichten, lernen Sie die allgemeinen Best Practices und Empfehlungen der Konfiguration kennen. So können Sie sicherstellen, dass Ihre FPolicy-Konfiguration

eine robuste Monitoring-Performance sowie Ergebnisse liefert, die Ihre Anforderungen erfüllen.

Arbeiten Sie mit Ihrer FPolicy-Partnerapplikation zusammen, um spezifische Richtlinien in Bezug auf Performance, Größenbestimmung und Konfiguration zu erhalten.

Persistente Speicher

Ab ONTAP 9.14.1 können Sie mit FPolicy einen persistenten Speicher einrichten, um Dateizugriffsereignisse für asynchrone, nicht obligatorische Richtlinien auf der SVM zu erfassen. Persistente Speicher können die Client-I/O-Verarbeitung von der FPolicy-Benachrichtigungsverarbeitung entkoppeln, um die Client-Latenz zu verringern. Synchrone (obligatorische oder nicht obligatorische) und asynchrone obligatorische Konfigurationen werden nicht unterstützt.

- Bevor Sie die Funktion „persistenter Speicher“ verwenden, stellen Sie sicher, dass Ihre Partneranwendungen diese Konfiguration unterstützen.
- Sie benötigen einen persistenten Speicher für jede SVM, auf 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, das zugehörige Volume und die zugehörige Volume-Konfiguration werden bei der Erstellung des persistenten Speichers automatisch übernommen.
- ONTAP 9.14.1:
  - Der persistente Speicher, das zugehörige Volume und die Volume-Konfiguration werden manuell übernommen.
- Erstellen Sie das persistente Speicher-Volume auf dem Node mit LIFs, die davon ausgehen, dass der maximale Datenverkehr durch 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 ein Volume für den persistenten Speicher jeder SVM erstellen und konfigurieren, auf der FPolicy aktiviert ist.
- Wenn die im persistenten Speicher angesammelten Benachrichtigungen die Größe des bereitgestellten Volumes überschreiten, beginnt FPolicy die eingehende Benachrichtigung mit den entsprechenden EMS-Nachrichten zu löschen.
  - ONTAP 9.15.1 oder höher: Zusätzlich zum `size` Parameter `autosize-mode` kann der Parameter dem Wachstum oder Verkleinern des Volumes als Antwort auf die Menge des genutzten Speicherplatzes helfen.
  - ONTAP 9.14.1: Der `size` Parameter wird während der Volume-Erstellung so konfiguriert, dass er ein maximales Limit bietet.
- Setzen Sie die Snapshot-Policy auf `none` für das persistente Speichervolumen statt auf `default` . Dadurch wird sichergestellt, dass keine versehentliche Wiederherstellung des Snapshots zum Verlust aktueller Ereignisse führt und eine mögliche doppelte Ereignisverarbeitung verhindert wird.
  - ONTAP 9.15.1 oder höher: Der `snapshot-policy` Parameter wird während der Erstellung eines persistenten Speichers automatisch auf none konfiguriert.
  - ONTAP 9.14.1: Der `snapshot-policy` Parameter wird `none` während der Volume-Erstellung auf konfiguriert.
- Machen Sie das persistente Speicher-Volume für den externen Zugriff auf das Benutzerprotokoll

(CIFS/NFS) unzugänglich, um versehentliche Beschädigungen oder das Löschen von permanenten Ereignisdatensätzen zu vermeiden.

  - ONTAP 9.15.1 oder höher: ONTAP blockiert das Volume während der Erstellung des persistenten Speichers automatisch aus externem Benutzerprotokollzugriff (CIFS/NFS).
  - ONTAP 9.14.1: Heben Sie nach der Aktivierung von FPolicy die Bereitstellung des Volumes in ONTAP auf, um den Verbindungspfad zu entfernen. Dies macht es für externen Benutzer-Protokoll-Zugriff (CIFS/NFS) unzugänglich.

Weitere Informationen finden Sie unter "FPolicy persistente Speicher" und "Erstellen persistenter Speicher".

Persistentes Failover und Giveback von Speichern

Der persistente Speicher bleibt so, wie er zu dem Zeitpunkt empfangen wurde, wenn ein unerwartetes Neubooten angezeigt wird oder FPolicy wird deaktiviert und erneut aktiviert. Nach einem Übernahmevorgang werden neue Ereignisse gespeichert und vom Partner-Node verarbeitet. Nach einem Giveback-Vorgang setzt der persistente Speicher die Verarbeitung aller nicht verarbeiteten Ereignisse fort, die möglicherweise vom Zeitpunkt der Node-Übernahme entfernt bleiben. Live-Events würden Vorrang vor nicht verarbeiteten Ereignissen erhalten.

Wenn das persistente Speichervolume von einem Knoten zu einem anderen in derselben SVM verschoben wird, werden die noch zu verarbeitenden Benachrichtigungen ebenfalls auf den neuen Knoten verschoben. Sie müssen den `fpolicy persistent-store create` Befehl auf einem der Knoten, nachdem das Volume verschoben wurde, um sicherzustellen, dass die ausstehenden Benachrichtigungen an den externen Server übermittelt werden.

Erfahren Sie mehr über `fpolicy persistent-store create` im "ONTAP-Befehlsreferenz" .

Konfiguration von Richtlinien

Die Konfiguration der externen FPolicy Engine, Ereignisse und Umfang für SVMs können die Benutzerfreundlichkeit und die Sicherheit insgesamt verbessern.

- Konfiguration der FPolicy externen Engine für SVMs:
  - Zusätzliche Sicherheit ist mit Performance-Kosten verbunden. Die Aktivierung der SSL-Kommunikation (Secure Sockets Layer) wirkt sich auf die Leistung des Zugriffs auf Freigaben aus.
  - Die externe FPolicy Engine sollte mit mehr als einem FPolicy Server konfiguriert werden, um Ausfallsicherheit und Hochverfügbarkeit bei der Verarbeitung von FPolicy Serverbenachrichtigungen zu gewährleisten.
- Konfiguration von FPolicy Ereignissen für SVMs:

  Die Überwachung von Dateioperationen wirkt sich auf Ihre Gesamterfahrung aus. Das Filtern unerwünschter Dateioperationen auf der Storage-Seite verbessert beispielsweise die Benutzerfreundlichkeit. NetApp empfiehlt die Einrichtung der folgenden Konfiguration:

  - Überwachung der Mindestanforderungen an Dateioperationen und Aktivierung der maximalen Anzahl von Filtern ohne Unterbrechung des Anwendungsfalls.
  - Verwenden von Filtern für getattr-, Lese-, Schreib-, Öffnen- und Schließvorgänge. In den Home Directory-Umgebungen SMB und NFS kommt ein hoher Prozentsatz dieser Vorgänge zum Einsatz.
- Konfiguration des FPolicy Umfangs für SVMs:

  Schränken Sie die Richtlinien auf relevante Storage-Objekte wie Freigaben, Volumes und Exporte ein, anstatt sie über die gesamte SVM zu aktivieren. NetApp empfiehlt, die Verzeichniserweiterungen zu

überprüfen. Wenn der `is-file-extension-check-on-directories-enabled` Parameter auf gesetzt `true` ist, werden Verzeichnisobjekte denselben Erweiterungsprüfungen unterzogen wie normale Dateien.

Netzwerkkonfiguration

Die Netzwerkverbindung zwischen dem FPolicy-Server und dem Controller sollte geringe Latenz aufweisen. NetApp empfiehlt die Trennung des FPolicy-Datenverkehrs vom Client-Verkehr über ein privates Netzwerk.

Außerdem sollten sich externe FPolicy Server (FPolicy-Server) in der Nähe des Clusters mit hoher Bandbreite befinden, um minimale Latenz und Konnektivität mit hoher Bandbreite zu ermöglichen.

> In einem Szenario, in dem die LIF für FPolicy-Datenverkehr auf einem anderen Port zur LIF für Client-Datenverkehr konfiguriert wird, kann die FPolicy LIF aufgrund eines Portausfalls einen Failover auf den anderen Node durchführen. Infolgedessen kann der FPolicy-Server von dem Node nicht mehr erreicht werden, was dazu führt, dass die FPolicy-Benachrichtigungen für Dateivorgänge auf dem Node fehlschlagen. Um dieses Problem zu vermeiden, überprüfen Sie, ob der FPolicy-Server über mindestens eine logische Schnittstelle auf dem Node erreichbar ist, um FPolicy-Anfragen für die Dateivorgänge zu verarbeiten, die auf diesem Node ausgeführt werden.

Hardwarekonfiguration

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

Das Cluster-Node-to-FPolicy-Serververhältnis sollte optimiert werden, um sicherzustellen, dass FPolicy Server nicht überlastet sind. Dies kann Latenzen bedeuten, wenn die SVM auf Client-Anforderungen reagiert. Das optimale Verhältnis hängt von der Partnerapplikation ab, für die der FPolicy-Server verwendet wird. NetApp empfiehlt die Zusammenarbeit mit Partnern, um den geeigneten Wert zu ermitteln.

Konfiguration mehrerer Richtlinien

Die FPolicy-Richtlinie für natives Blockieren hat unabhängig von der Sequenznummer die höchste Priorität und Richtlinien zur Änderung der Entscheidungsfindung haben eine höhere Priorität als andere. Die Priorität der Richtlinie hängt von dem jeweiligen Anwendungsfall ab. NetApp empfiehlt die Zusammenarbeit mit Partnern, um die entsprechende Priorität zu bestimmen.

Überlegungen zur Größe

FPolicy überwacht SMB- und NFS-Vorgänge inline, sendet Benachrichtigungen an den externen Server und wartet je nach Kommunikationsmodus der externen Engine (synchron oder asynchron) auf eine Antwort. Dieser Prozess wirkt sich auf die Performance von SMB- und NFS-Zugriffs- sowie CPU-Ressourcen aus.

Um Probleme zu beheben, empfiehlt NetApp, gemeinsam mit Partnern die Umgebung zu bewerten und zu dimensionieren, bevor FPolicy aktiviert wird. Die Performance wird von verschiedenen Faktoren beeinflusst, darunter die Benutzeranzahl und Workload-Merkmale wie Vorgänge pro Benutzer und Datengröße, Netzwerklatenz sowie Ausfall- oder Server-Langsamkeit.

Monitoring der Performance

FPolicy ist ein auf Benachrichtigungen basierendes System. Benachrichtigungen werden zur Verarbeitung an

einen externen Server gesendet, um eine Antwort an ONTAP zu generieren. Durch diesen Round-Trip-Prozess erhöht sich die Latenz für den Client-Zugriff.

Durch das Monitoring der Performance-Zähler auf dem FPolicy-Server und in ONTAP können Engpässe in der Lösung identifiziert und die Parameter nach Bedarf für eine optimale Lösung angepasst werden. Eine Zunahme der FPolicy-Latenz wirkt sich beispielsweise kaskadierend auf die Latenz des SMB- und NFS-Zugriffs aus. Daher sollten Sie sowohl die Workload- (SMB und NFS) als auch die FPolicy-Latenz überwachen. Zudem können Sie mithilfe von Quality-of-Service-Richtlinien in ONTAP einen Workload für jedes Volume oder jede SVM einrichten, die für FPolicy aktiviert ist.

NetApp empfiehlt, den `statistics show –object workload` Befehl zum Anzeigen von Workload-Statistiken auszuführen. Außerdem sollten Sie die folgenden Parameter überwachen:

- Durchschnittliche Lese-, Schreib- und Leselatenz
- Gesamtzahl der Vorgänge
- Zähler lesen und schreiben

Die Performance von FPolicy-Subsystemen kann mit den folgenden FPolicy-Zählern überwacht werden.

Sie müssen sich im Diagnosemodus befinden, um Statistiken zu FPolicy zu sammeln.

Schritte

1. FPolicy-Zähler sammeln:
   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` `fpolicy_server` Zähler und bieten Informationen zu verschiedenen Leistungsparametern, die in der folgenden Tabelle beschrieben sind.

Zähler	Beschreibung
fpolicy-Zähler	Abgebrochene_Anforderungen
Anzahl der Bildschirmanforderungen, für die die Verarbeitung auf der SVM abgebrochen wird	Event_count
Liste der Ereignisse, die zu einer Benachrichtigung führen	max_request_Latenz

Zähler	Beschreibung
Maximale Verzögerung bei Bildschirmanforderungen	Ausstehende_Anforderungen
Gesamtanzahl der in Bearbeitung vorhandenen Bildschirmanforderungen	Verarbeitete_Anforderungen
Gesamtzahl der Bildschirmanforderungen, die die fpolicy-Verarbeitung auf der SVM durchlaufen haben	Request_Latency_hist
Histogramm der Latenz für Bildschirmanforderungen	Requests_sended_Rate
Anzahl der pro Sekunde versandten Bildschirmanfragen	Requests_received_Rate
Anzahl der empfangenen Bildschirmanforderungen pro Sekunde	**fpolicy_Server-Zähler**
max_request_Latenz	Maximale Latenz für eine Bildschirmanforderung
Ausstehende_Anforderungen	Gesamtzahl der auf Antwort wartenden Bildschirmanforderungen
Request_Latency	Durchschnittliche Latenz für Bildschirmanforderung
Request_Latency_hist	Histogramm der Latenz für Bildschirmanforderungen
Request_sent_Rate	Anzahl der an den FPolicy-Server gesendeten Bildschirmanfragen pro Sekunde
Response_received_Rate	Anzahl der vom FPolicy-Server empfangenen Bildschirmantworten pro Sekunde

Erfahren Sie mehr über `statistics start` und `statistics show` in der "ONTAP-Befehlsreferenz".

Managen Sie FPolicy Workflows und Abhängigkeit von anderen Technologien

NetApp empfiehlt, eine FPolicy-Richtlinie zu deaktivieren, bevor Sie Konfigurationsänderungen vornehmen. Wenn Sie beispielsweise eine IP-Adresse in der externen Engine hinzufügen oder ändern möchten, die für die aktivierte Richtlinie konfiguriert ist, deaktivieren Sie zunächst die Richtlinie.

Wenn Sie FPolicy zur Überwachung von NetApp FlexCache Volumes konfigurieren, empfiehlt NetApp, FPolicy nicht für die Überwachung von Lese- und getattr-Dateivorgängen zu konfigurieren. Zur Überwachung dieser

Vorgänge in ONTAP ist der Abruf von I2P-Daten (Inode-to-Path) erforderlich. Da die I2P-Daten nicht von FlexCache-Volumes abgerufen werden können, müssen sie vom Ursprungs-Volume abgerufen werden. Daher eliminiert das Monitoring dieser Operationen die Performance-Vorteile, die FlexCache bieten kann.

Wenn FPolicy und eine Off-Box-Antivirus-Lösung implementiert werden, erhält die Virenschutzlösung zuerst Benachrichtigungen. Die FPolicy-Verarbeitung wird erst gestartet, nachdem die Virenprüfung abgeschlossen ist. Es ist wichtig, dass Sie Virenschutzlösungen korrekt dimensionieren, da ein langsamer Virenschutzscanner die Gesamtleistung beeinträchtigen kann.

Überlegungen zum Passthrough-Upgrade und Zurücksetzen

Es gibt bestimmte Überlegungen zum Upgrade und Zurücksetzen, die Sie vor dem Upgrade auf eine ONTAP-Version, die Passthrough-Read unterstützt, oder vor dem Zurücksetzen auf eine Version ohne Passthrough-Read wissen müssen.

Aktualisierung

Nachdem alle Knoten auf eine Version von ONTAP aktualisiert wurden, die FPolicy PassThrough-Read unterstützt, kann der Cluster die Passthrough-Read-Funktion nutzen; allerdings ist Passthrough-read bei bestehenden FPolicy-Konfigurationen standardmäßig deaktiviert. Um Passthrough-read für bestehende FPolicy-Konfigurationen zu verwenden, müssen Sie die FPolicy deaktivieren und die Konfiguration ändern und dann die Konfiguration erneut aktivieren.

Zurücksetzen

Bevor Sie auf eine Version von ONTAP zurücksetzen, die FPolicy Passthrough-Read nicht unterstützt, müssen Sie die folgenden Bedingungen erfüllen:

- Deaktivieren Sie alle Richtlinien mit Passthrough-read, und ändern Sie dann die betroffenen Konfigurationen, sodass sie keine Passthrough-Read-Einstellungen verwenden.
- Deaktivieren Sie FPolicy-Funktionen auf dem Cluster, indem Sie alle FPolicy-Richtlinien auf dem Cluster deaktivieren.

Bevor Sie auf eine Version von ONTAP zurücksetzen, die persistente Speicher nicht unterstützt, stellen Sie sicher, dass keine der FPolicy-Richtlinien über einen konfigurierten persistenten Speicher verfügt. Wenn ein persistenter Speicher konfiguriert ist, schlägt die Wiederherstellung fehl.

Verwandte Informationen

- "Statistiken zeigen"
- "Statistikstart"

Einrichten von ONTAP FPolicy-Konfigurationen

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

Die folgenden Schritte zum Einrichten und Aktivieren einer FPolicy-Konfiguration auf der SVM sind:

1. Erstellen einer externen FPolicy Engine.

   Die externe FPolicy Engine identifiziert die externen FPolicy Server (FPolicy Server), die mit einer

bestimmten FPolicy-Konfiguration assoziiert sind. Wenn die interne „`native` FPolicy Engine“ verwendet wird, um eine native File-Blocking-Konfiguration zu erstellen, müssen Sie keine FPolicy-externe Engine erstellen.

Ab ONTAP 9.15.1 können Sie das `protobuf` Engine-Format verwenden. Wenn auf eingestellt `protobuf`, werden die Benachrichtigungen in binärer Form mit Google protobuf codiert. Bevor Sie das Engine-Format auf setzen `protobuf`, stellen Sie sicher, dass der FPolicy-Server auch `protobuf` Deserialisierung unterstützt. Weitere Informationen finden Sie unter "Planen Sie die Konfiguration der externen FPolicy Engine"

2. Erstellen eines FPolicy-Ereignisses.

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

3. Erstellen eines persistenten FPolicy-Speichers (optional)

   Ab ONTAP 9.14.1 können Sie mit FPolicy "Persistente Speicher"Dateizugriffsereignisse für asynchrone, nicht obligatorische Richtlinien in der SVM erfassen. Synchrone (obligatorische oder nicht obligatorische) und asynchrone obligatorische Konfigurationen werden nicht unterstützt.

   Persistente Speicher können die Client-I/O-Verarbeitung von der FPolicy-Benachrichtigungsverarbeitung entkoppeln, um die Client-Latenz zu verringern.

   Ab ONTAP 9.15.1 wird die Konfiguration persistenter FPolicy-Speicher vereinfacht. Der `persistent-store-create` Befehl automatisiert die Volume-Erstellung für die SVM und konfiguriert das Volume für den persistenten Speicher.

4. Erstellen einer FPolicy.

   Die FPolicy ist dafür verantwortlich, mit dem entsprechenden Umfang die zu überwachenden Ereignisse zu verknüpfen und für welche der überwachten Ereignisse Benachrichtigungen an den designierten FPolicy-Server (oder an die native Engine gesendet werden müssen, wenn keine FPolicy-Server konfiguriert sind). Die Richtlinie legt außerdem fest, ob der FPolicy-Server privilegierten Zugriff auf die Daten gewährt, für die er Benachrichtigungen erhält. Ein FPolicy-Server benötigt privilegierten Zugriff, wenn der Server auf die Daten zugreifen muss. Typische Anwendungsfälle, in denen privilegierter Zugriff erforderlich ist, sind das File Blocking, das Kontingentmanagement und das hierarchische Storage-Management. Mit der Richtlinie legen Sie fest, ob die Konfiguration für diese Richtlinie einen FPolicy-Server oder den internen „`nativen` FPolicy Server“ verwendet.

   Eine Richtlinie gibt an, ob das Screening erforderlich ist. Wenn das Screening zwingend erforderlich ist und alle FPolicy Server ausgefallen sind oder keine Antwort von den FPolicy-Servern innerhalb eines definierten Zeitlimits erhalten wird, wird der Dateizugriff verweigert.

   Die Grenzen einer Richtlinie sind die SVM. Eine Richtlinie kann nicht auf mehr als eine SVM angewendet werden. Für eine bestimmte SVM können jedoch mehrere FPolicy-Richtlinien gelten, wobei jedes einzelne von der gleichen oder einer anderen Kombination aus Scope-, Ereignis- und externen Serverkonfigurationen aufweisen kann.

5. Konfigurieren des Richtlinienumfangs.

   Der FPolicy-Umfang legt fest, welche Volumes, Shares oder Exportrichtlinien die Richtlinie für das

Monitoring agiert oder nicht. Ein Umfang legt auch fest, welche Dateiendungen vom FPolicy Monitoring enthalten oder ausgeschlossen werden sollten.

> Ausschlusslisten haben Vorrang vor include-Listen.

6. Aktivieren Sie die FPolicy.

   Wenn die Richtlinie aktiviert ist, werden die Kontrollkanäle und optional die privilegierten Datenkanäle verbunden. Der FPolicy-Prozess auf den Nodes, an denen die SVM teilnimmt, beginnt mit der Überwachung der Datei- und Ordnerzugriff und sendet bei Ereignissen, die konfigurierte Kriterien erfüllen, Benachrichtigungen an die FPolicy Server (oder an die native Engine, wenn keine FPolicy-Server konfiguriert sind).

> Wenn die Richtlinie die native Blockierung von Dateien verwendet, wird eine externe Engine nicht konfiguriert oder mit der Richtlinie verknüpft.

Planen Sie die Konfiguration der externen FPolicy Engine

Planen Sie die Konfigurationen externer ONTAP FPolicy-Engines

Bevor Sie die externe FPolicy Engine konfigurieren, müssen Sie wissen, was es bedeutet, eine externe Engine zu erstellen, und welche Konfigurationsparameter verfügbar sind. Anhand dieser Informationen können Sie festlegen, welche Werte für jeden Parameter festgelegt werden sollen.

Informationen, die bei der Erstellung der externen FPolicy Engine definiert werden

Die Konfiguration der externen Engine definiert die Informationen, die FPolicy benötigt, um Verbindungen zu den externen FPolicy Servern herzustellen und zu managen, darunter:

- SVM-Name
- Motorname
- Die IP-Adressen der primären und sekundären FPolicy Server und der zu verwendenden TCP-Portnummer für die Verbindung zu den FPolicy Servern
- Ob der Engine-Typ asynchron oder synchron ist
- Gibt an, ob das Motorformat `xml` oder ist `protobuf`

  Ab ONTAP 9.15.1 können Sie das `protobuf` Engine-Format verwenden. Wenn auf eingestellt `protobuf`, werden die Benachrichtigungen in binärer Form mit Google protobuf codiert. Bevor Sie das Engine-Format auf setzen `protobuf`, stellen Sie sicher, dass der FPolicy-Server auch `protobuf` Deserialisierung unterstützt.

  Da das Protobuf-Format ab ONTAP 9.15.1 unterstützt wird, müssen Sie das externe Engine-Format berücksichtigen, bevor Sie zu einer früheren Version von ONTAP zurückkehren. Wenn Sie eine ältere Version als ONTAP 9.15.1 wiederherstellen, arbeiten Sie mit Ihrem FPolicy-Partner zusammen, um einen der folgenden Schritte auszuführen:

  - Ändern Sie jedes Motorformat von `protobuf` in `xml`

    - Löschen Sie die Engines mit dem Motorformat `protobuf`
- Wie authentifiziert man die Verbindung zwischen dem Knoten und dem FPolicy-Server

  Wenn Sie die gegenseitige SSL-Authentifizierung konfigurieren, müssen Sie auch Parameter konfigurieren, die SSL-Zertifikatsinformationen bereitstellen.

- So verwalten Sie die Verbindung mit verschiedenen erweiterten Berechtigungseinstellungen

  Dazu gehören Parameter, die z. B. Timeout-Werte, Wiederholungswerte, Keep-Alive-Werte, maximale Anforderungswerte, Werte für gesendete und empfangbare Puffergrößen sowie Werte für Sitzungszeitüberschreitungen definieren.

Mit dem `vserver fpolicy policy external-engine create` Befehl wird eine externe FPolicy Engine erstellt.

Was sind die grundlegenden externen Motorparameter

Sie können die folgende Tabelle mit grundlegenden FPolicy Konfigurationsparametern verwenden, um Ihre Konfiguration zu planen:

Informationstyp	Option
SVM Gibt den SVM-Namen an, den Sie mit dieser externen Engine verknüpfen möchten. Jede FPolicy-Konfiguration ist innerhalb einer einzelnen SVM definiert. Die externe Engine, das Richtlinienereignis, der Richtlinienumfang und die Richtlinie, die gemeinsam eine FPolicy-Konfiguration erstellen, müssen mit derselben SVM verknüpft werden.	`-vserver vserver_name`

Motorname Gibt den Namen an, der der externen Engine-Konfiguration zugewiesen werden soll. Sie müssen den Namen der externen Engine später angeben, wenn Sie die FPolicy erstellen. Dadurch wird die externe Engine mit der Richtlinie verknüpft. Der Name kann bis zu 256 Zeichen lang sein. Wenn Sie den Namen der externen Engine in einer Disaster-Recovery-Konfiguration von MetroCluster oder SVM konfigurieren, sollte der Name bis zu 200 Zeichen lang sein. Der Name kann eine beliebige Kombination der folgenden Zeichen des ASCII-Bereichs enthalten: • `a` Durch `z` • `A` Durch `Z` • `0` Durch `9` • „_“, „-`", and ".`“	`-engine-name engine_name`
Primary FPolicy Server Gibt die primären FPolicy Server an, an die der Node Benachrichtigungen für eine bestimmte FPolicy sendet. Der Wert wird als kommagetrennte Liste von IP-Adressen angegeben. Wenn mehr als eine IP-Adresse für den primären Server angegeben wird, erstellt jeder Node, an dem die SVM teilnimmt, eine Kontrollverbindung zu jedem angegebenen primären FPolicy-Server zum Zeitpunkt der Aktivierung der Richtlinie. Wenn Sie mehrere primäre FPolicy-Server konfigurieren, werden Benachrichtigungen nach Round Robin-Verfahren an die FPolicy-Server gesendet. Wenn die externe Engine in einer MetroCluster- oder SVM-Disaster-Recovery-Konfiguration verwendet wird, sollten Sie die IP-Adressen der FPolicy-Server am Quellstandort als primäre Server angeben. 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`

Secondary FPolicy Server Gibt die sekundären FPolicy-Server an, an die Dateizugriffsereignisse für eine bestimmte FPolicy gesendet werden sollen. Der Wert wird als kommagetrennte 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. Benachrichtigungen werden jedoch nur an sekundäre Server gesendet, wenn keiner der primären Server erreichbar ist. Wenn Sie mehrere sekundäre Server konfigurieren, werden Benachrichtigungen nach Round Robin-Verfahren an die FPolicy-Server gesendet.	`-secondary-servers IP_address,...`
Externer Motortyp Gibt an, ob die externe Engine im synchronen oder asynchronen Modus arbeitet. FPolicy arbeitet standardmäßig im synchronen Modus. Wenn auf eingestellt `synchronous`, sendet die Dateianforderungsverarbeitung eine Benachrichtigung an den FPolicy-Server, wird jedoch erst fortgesetzt, nachdem eine Antwort vom FPolicy-Server empfangen wurde. In diesem Punkt wird der Anforderungsfluss entweder fortgesetzt oder die Verarbeitung führt zu Denial-DoS, je nachdem, ob die Antwort vom FPolicy-Server die angeforderte Aktion zulässt. Wenn auf festgelegt `asynchronous`, sendet die Dateianforderungsverarbeitung eine Benachrichtigung an den FPolicy-Server und fährt dann fort.	`-extern-engine-type external_engine_type` Der Wert für diesen Parameter kann einer der folgenden sein: • `synchronous` • `asynchronous`
Format der externen Engine Geben Sie an, ob das Format der externen Engine XML oder protobuf ist. Ab ONTAP 9.15.1 können Sie das protobuf-Engine-Format verwenden. Wenn auf protobuf gesetzt, werden die Benachrichtigungen in binärer Form mit Google protobuf codiert. Bevor Sie das Engine-Format auf Protobuf setzen, stellen Sie sicher, dass der FPolicy Server auch die Protobuf-Deserialisierung unterstützt.	`- extern-engine-format` {`protobuf` Oder `xml`}

SSL-Option zur Kommunikation mit FPolicy Server Gibt die SSL-Option für die Kommunikation mit dem FPolicy-Server an. Dies ist ein erforderlicher Parameter. Sie können eine der Optionen basierend auf den folgenden Informationen auswählen: • Wenn auf eingestellt `no-auth`, findet keine Authentifizierung statt. Die Kommunikationsverbindung wird über TCP hergestellt. • Wenn auf festgelegt `server-auth`, authentifiziert die SVM den FPolicy-Server mithilfe von SSL-Serverauthentifizierung. • Bei Einstellung auf `mutual-auth` erfolgt die gegenseitige Authentifizierung zwischen SVM und FPolicy-Server. Die SVM authentifiziert den FPolicy-Server und der FPolicy-Server authentifiziert die SVM. Wenn Sie die gegenseitige SSL-Authentifizierung konfigurieren möchten, müssen Sie auch die `-certificate-common-name -certificate-serial -certifcate-ca` Parameter , und konfigurieren.	`-ssl-option` {`no-auth`
`server-auth`	`mutual-auth`}
Zertifikat FQDN oder benutzerdefinierter allgemeiner Name Gibt den Zertifikatsnamen an, der verwendet wird, wenn die SSL-Authentifizierung zwischen der SVM und dem FPolicy-Server konfiguriert ist. Sie können den Zertifikatnamen als FQDN oder als benutzerdefinierten gemeinsamen Namen angeben. Wenn Sie `mutual-auth` für den `-ssl-option` Parameter angeben, müssen Sie einen Wert für den `-certificate-common-name` Parameter angeben.	`-certificate-common -name` `text`
Seriennummer des Zertifikats Gibt die Seriennummer des Zertifikats an, das für die Authentifizierung verwendet wird, wenn die SSL-Authentifizierung zwischen der SVM und dem FPolicy-Server konfiguriert ist. Wenn Sie `mutual-auth` für den `-ssl-option` Parameter angeben, müssen Sie einen Wert für den `-certificate-serial` Parameter angeben.	`-certificate-serial` `text`

Zertifizierungsstelle Gibt den CA-Namen des Zertifikats an, das für die Authentifizierung verwendet wird, wenn die SSL-Authentifizierung zwischen der SVM und dem FPolicy-Server konfiguriert ist. Wenn Sie `mutual-auth` für den `-ssl-option` Parameter angeben, müssen Sie einen Wert für den `-certificate-ca` Parameter angeben.	`-certificate-ca text`

Was sind die erweiterten Optionen der externen Engine

Sie können die folgende Tabelle mit erweiterten FPolicy Konfigurationsparametern verwenden, wenn Sie planen, Ihre Konfiguration mit erweiterten Parametern anzupassen. Mit diesen Parametern ändern Sie das Kommunikationsverhalten zwischen den Cluster-Nodes und den FPolicy-Servern:

Informationstyp	Option
Timeout zum Abbrechen einer Anfrage Gibt das Zeitintervall in hours (`h`)(`m`(`s`, minutes) oder seconds) an, das der Knoten auf eine Antwort vom FPolicy-Server wartet. Wenn das Zeitüberschreitungsintervall abgelaufen ist, sendet der Node eine Anforderung zum Abbrechen an den FPolicy-Server. Der Node sendet dann die Benachrichtigung an einen alternativen FPolicy-Server. Dieses Timeout unterstützt den Umgang mit einem FPolicy-Server, der nicht reagiert, was die Reaktion von SMB/NFS-Clients verbessern kann. Das Abbrechen von Anfragen nach einem Timeout kann außerdem dazu beitragen, Systemressourcen freizugeben, da die Benachrichtigungsanfrage von einem heruntergedrückten/schlechten FPolicy-Server auf einen alternativen FPolicy-Server verschoben wird. Der Bereich für diesen Wert ist `0` bis `100`. Wenn der Wert auf festgelegt `0` ist, ist die Option deaktiviert und Abbruchmeldungen werden nicht an den FPolicy-Server gesendet. Der Standardwert ist `20s`.	`-reqs-cancel-timeout integer`[M]
Timeout für Abbruch einer Anfrage Gibt das Timeout in hours (`h`), minutes) (`m`` oder seconds (`s`) für den Abbruch einer Anfrage an. Der Bereich für diesen Wert ist `0` bis `200`.	`-reqs-abort-timeout ` `integer`[M]
Intervall für das Senden von Statusanforderungen Gibt das Intervall in Stunden (`h`), Minuten (`m`) oder Sekunden (`s`) an, nach dem eine Statusanfrage an den FPolicy-Server gesendet wird. Der Bereich für diesen Wert ist `0` bis `50`. Wenn der Wert auf festgelegt `0` ist, ist die Option deaktiviert und Statusanforderungsmeldungen werden nicht an den FPolicy-Server gesendet. Der Standardwert ist `10s`.	`-status-req-interval integer`[M]

Maximale Anzahl ausstehende Anforderungen auf dem FPolicy-Server Gibt die maximale Anzahl der ausstehenden Anforderungen an, die auf dem FPolicy-Server in die Warteschlange gestellt werden können. Der Bereich für diesen Wert ist `1` bis `10000`. Der Standardwert ist `500`.	`-max-server-reqs integer`
Timeout zum Trennen eines nicht ansprechenden FPolicy Servers 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 dem Timeout-Zeitraum nur beendet, wenn die Warteschlange des FPolicy-Servers die maximal zulässigen Anforderungen enthält und innerhalb des Timeout-Zeitraums keine Antwort empfangen wird. Die maximal zulässige Anzahl von Anforderungen ist entweder `50` (Standard) oder die vom `max-server-reqs-` Parameter angegebene Anzahl. Der Bereich für diesen Wert ist `1` bis `100`. Der Standardwert ist `60s`.	`-server-progress -timeout integer`[M]
Intervall zum 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-Meldungen erkennen halboffene Verbindungen. Der Bereich für diesen Wert ist `10` bis `600`. Wenn der Wert auf festgelegt `0` ist, wird die Option deaktiviert und Keep-Alive-Nachrichten werden nicht an die FPolicy-Server gesendet. Der Standardwert ist `120s`.	`-keep-alive-interval- integer`[M]
Maximale Anzahl Verbindungsversuche Gibt die maximale Anzahl der Male an, die die SVM nach einer Verbindungsherstellung versucht, eine Verbindung zum FPolicy-Server herzustellen. Der Bereich für diesen Wert ist `0` bis `20`. Der Standardwert ist `5`.	`-max-connection-retries integer`

Puffergröße empfangen Gibt die Empfangsbuffer-Größe des angeschlossenen Sockets für den FPolicy-Server an. Der Standardwert ist 256 Kilobyte (KB). Wenn der Wert auf 0 gesetzt ist, wird die Größe des Empfangspuffers auf einen vom System definierten Wert gesetzt. Wenn beispielsweise die Standard-Empfangspuffgröße des Sockets 65536 Byte beträgt, wird durch Setzen des einstellbaren Werts auf 0 die Socket-Puffergröße auf 65536 Byte gesetzt. Sie können einen beliebigen nicht-Standardwert verwenden, um die Größe (in Byte) des Empfangspuffers festzulegen.	`-recv-buffer-size integer`
Puffergröße senden Gibt die Sendepuffer-Größe des angeschlossenen Sockets für den FPolicy-Server an. Der Standardwert ist 256 Kilobyte (KB). Wenn der Wert auf 0 gesetzt ist, wird die Größe des Sendepuffers auf einen vom System definierten Wert gesetzt. Wenn beispielsweise die Standard-Sendepuffer-Größe des Sockets auf 65536 Byte eingestellt ist, indem der einstellbare Wert auf 0 gesetzt wird, wird die Socket-Puffergröße auf 65536 Byte gesetzt. Sie können einen beliebigen nicht-Standardwert verwenden, um die Größe (in Bytes) des Sendepuffers festzulegen.	`-send-buffer-size integer`
Timeout zum Löschen einer Sitzungs-ID während der erneuten Verbindung Gibt das Intervall in hours (`h`), minutes) (`m`oder seconds (`s`) an, nach dem während der Verbindungsversuche eine neue Session ID an den FPolicy-Server gesendet wird. Wenn die Verbindung zwischen dem Storage-Controller und dem FPolicy-Server beendet wird und innerhalb des `-session-timeout` Intervalls eine erneute Verbindung hergestellt wird, wird die alte Session ID an den FPolicy-Server gesendet, sodass sie Antworten auf alte Benachrichtigungen senden kann. Der Standardwert ist 10 Sekunden.	`-session-timeout [integerH][integerm][integers]`

Zusätzliche Informationen zum Konfigurieren externer ONTAP FPolicy-Engines zur Verwendung von SSL-authentifizierten Verbindungen

Sie müssen einige zusätzliche Informationen wissen, wenn Sie die FPolicy externe Engine konfigurieren möchten, um SSL bei der Verbindung zu FPolicy-Servern zu verwenden.

SSL-Serverauthentifizierung

Wenn Sie die FPolicy-externe Engine für die SSL-Server-Authentifizierung konfigurieren, müssen Sie vor dem Erstellen der externen Engine das öffentliche Zertifikat der Zertifizierungsstelle (CA) installieren, die das FPolicy-Server-Zertifikat signiert hat.

Gegenseitige Authentifizierung

Wenn Sie FPolicy externe Engines konfigurieren, um bei der Verbindung von Storage Virtual Machine (SVM)-Daten-LIFs mit externen FPolicy-Servern SSL gegenseitige Authentifizierung zu verwenden, bevor Sie die externe Engine erstellen, Sie müssen das öffentliche Zertifikat der CA installieren, die das FPolicy-Serverzertifikat unterzeichnet hat, sowie das öffentliche Zertifikat und die Schlüsseldatei zur Authentifizierung der SVM. Löschen Sie dieses Zertifikat nicht, während FPolicy-Richtlinien das installierte Zertifikat verwenden.

Wenn das Zertifikat gelöscht wird, während FPolicy es für gegenseitige Authentifizierung verwendet, wenn eine Verbindung zu einem externen FPolicy-Server hergestellt wird, können Sie eine deaktivierte FPolicy, die dieses Zertifikat verwendet, nicht aktivieren. Die FPolicy kann in dieser Situation nicht wieder aktiviert werden, auch wenn ein neues Zertifikat mit denselben Einstellungen erstellt und auf der SVM installiert wird.

Wenn das Zertifikat gelöscht wurde, müssen Sie ein neues Zertifikat installieren, neue FPolicy-externe Engines erstellen, die das neue Zertifikat verwenden, und die neuen externen Engines mit der FPolicy verknüpfen, die Sie durch Ändern der FPolicy erneut aktivieren möchten.

Installieren Sie Zertifikate für SSL

Das öffentliche Zertifikat der CA, mit dem das FPolicy-Serverzertifikat signiert wird, wird mit dem `security certificate install` Befehl mit dem `-type` Parameter auf installiert `client-ca`. Der private Schlüssel und das öffentliche Zertifikat, die für die Authentifizierung der SVM erforderlich sind, werden mit dem `security certificate install` Befehl mit dem `-type` Parameter set to installiert `server`.

Verwandte Informationen

- "Sicherheitszertifikat installieren"

ONTAP FPolicy-Zertifikate werden in SVM-Disaster-Recovery-Beziehungen mit einer Konfiguration ohne ID-Preserve nicht repliziert

Sicherheitszertifikate, die für die SSL-Authentifizierung verwendet werden, wenn Verbindungen zu FPolicy-Servern hergestellt werden, replizieren keine SVM-Disaster-Recovery-Ziele mit Konfigurationen, die keine ID-Preserve enthalten. Obwohl die externe FPolicy-Engine-Konfiguration auf der SVM repliziert wird, werden Sicherheitszertifikate nicht repliziert. Sie müssen die Sicherheitszertifikate manuell auf dem Ziel installieren.

Wenn Sie die Disaster-Recovery-Beziehung für SVM einrichten, `-identity-preserve` `snapmirror create` bestimmen die Konfigurationsdetails, die auf der Ziel-SVM repliziert werden, der für die Option des Befehls ausgewählte Wert.

Wenn Sie die `-identity-preserve` Option auf `true` (ID-preserve) festlegen, werden alle Einzelheiten zur FPolicy Konfiguration repliziert, einschließlich der Sicherheitszertifikatinformationen. Sie müssen die Sicherheitszertifikate nur auf dem Ziel installieren, wenn Sie die Option auf `false` (nicht-ID-preserve) setzen.

Verwandte Informationen

- "snapmirror erstellen"

Einschränkungen für clusterbezogene ONTAP FPolicy-externe Engines mit MetroCluster- und SVM-Disaster-Recovery-Konfigurationen

Sie können eine externe Cluster-Scoped FPolicy Engine erstellen, indem Sie die Cluster Storage Virtual Machine (SVM) der externen Engine zuweisen. Beim Erstellen einer externen Engine mit Cluster-Umfang in einer Disaster-Recovery-Konfiguration mit MetroCluster oder SVM gibt es jedoch bestimmte Einschränkungen bei der Auswahl der Authentifizierungsmethode, die die SVM für die externe Kommunikation mit dem FPolicy-Server verwendet.

Es gibt drei Authentifizierungsoptionen, die Sie bei der Erstellung von externen FPolicy-Servern wählen können: Keine Authentifizierung, SSL-Serverauthentifizierung und gegenseitige SSL-Authentifizierung. Obwohl die Auswahl der Authentifizierungsoption für den externen FPolicy-Server einer Daten-SVM nicht eingeschränkt ist, gibt es Einschränkungen bei der Erstellung einer externen Cluster-Scoped FPolicy Engine:

Konfiguration	Erlaubt?
Disaster Recovery mit MetroCluster oder SVM und eine externe Cluster-FPolicy-Scoped-Engine ohne Authentifizierung (SSL ist nicht konfiguriert)	Ja.
Disaster Recovery für MetroCluster oder SVM und eine externe Cluster-FPolicy Scoped Engine mit SSL-Server oder gegenseitige SSL-Authentifizierung	Nein

- Wenn eine externe Cluster-Scoped FPolicy Engine mit SSL-Authentifizierung vorhanden ist und Sie eine MetroCluster- oder SVM-Disaster-Recovery-Konfiguration erstellen möchten, müssen Sie diese externe Engine ändern, um keine Authentifizierung zu verwenden oder die externe Engine zu entfernen, bevor Sie die MetroCluster- oder SVM-Disaster Recovery-Konfiguration erstellen können.
- Falls die Disaster Recovery-Konfiguration von MetroCluster oder SVM bereits vorhanden ist, verhindert ONTAP die Erstellung einer externen FPolicy Engine mit Cluster-Umfang und SSL-Authentifizierung.

Vollständige Arbeitsblätter zur Konfiguration der externen ONTAP FPolicy-Engine

Mit diesem Arbeitsblatt können Sie die Werte aufzeichnen, die Sie während der Konfiguration der externen FPolicy Engine benötigen. Wenn ein Parameterwert erforderlich ist, müssen Sie vor der Konfiguration der externen Engine festlegen, welchen Wert für diese Parameter verwendet werden soll.

Informationen für eine grundlegende externe Engine-Konfiguration

Sie sollten aufzeichnen, ob Sie die einzelnen Parametereinstellungen in die externe Engine-Konfiguration aufnehmen möchten, und dann den Wert für die Parameter notieren, die Sie einbeziehen möchten.

Informationstyp	Erforderlich	Einschließlich	Ihre Werte
Name der Storage Virtual Machine (SVM	Ja.	Ja.	
Motorname	Ja.	Ja.	

Primäre FPolicy-Server	Ja.	Ja.	
Port-Nummer	Ja.	Ja.	
Sekundäre FPolicy Server	Nein		
Externer Motortyp	Nein		
SSL-Option zur Kommunikation mit externem FPolicy-Server	Ja.	Ja.	
FQDN des Zertifikats oder benutzerdefinierter allgemeiner Name	Nein		
Seriennummer des Zertifikats	Nein		
Zertifizierungsstelle	Nein		

Informationen für erweiterte externe Motorparameter

Um eine externe Engine mit erweiterten Parametern zu konfigurieren, müssen Sie den Konfigurationsbefehl im erweiterten Berechtigungsmodus eingeben.

Informationstyp	Erforderlich	Einschließlich	Ihre Werte
Zeitüberschreitung beim Abbrechen einer Anfrage	Nein		
Timeout beim Abbrechen einer Anfrage	Nein		
Intervall für das Senden von Statusanforderungen	Nein		
Maximale offene Anfragen auf dem FPolicy-Server	Nein		
Timeout zum Trennen eines nicht ansprechenden FPolicy-Servers	Nein		
Intervall für das Senden von Keep-Alive-Nachrichten an den FPolicy-Server	Nein		
Maximale Anzahl von Verbindungsversuchen	Nein		
Empfangspuffgröße	Nein		

Puffergröße senden	Nein		
Zeitüberschreitung beim Spülen einer Sitzungs-ID während der erneuten Verbindung	Nein		

Planen Sie die FPolicy Event-Konfiguration

Erfahren Sie mehr über die ONTAP FPolicy Ereigniskonfiguration

Bevor Sie FPolicy-Ereignisse konfigurieren, müssen Sie verstehen, was es bedeutet, ein FPolicy-Ereignis zu erstellen. Sie müssen festlegen, welche Protokolle das Ereignis überwachen soll, welche Ereignisse überwacht werden sollen und welche Ereignisfilter verwendet werden sollen. Mit diesen Informationen können Sie die Werte planen, die Sie festlegen möchten.

Was es bedeutet, ein FPolicy-Ereignis zu erstellen

Erstellen des FPolicy-Ereignisses bedeutet, Informationen zu definieren, die der FPolicy-Prozess bestimmen muss, welche Dateizugriffsvorgänge überwacht werden und für welche der überwachten Ereignisse Benachrichtigungen an den externen FPolicy-Server gesendet werden sollen. Die FPolicy-Event-Konfiguration definiert die folgenden Konfigurationsinformationen:

- Name der Storage Virtual Machine (SVM
- Ereignis-Name
- Welche Protokolle zu überwachen sind

  FPolicy überwacht SMB, NFSv3, NFSv4 und – ab ONTAP 9.15.1 – NFSv4.1-Dateizugriffsvorgänge.

- Welche Dateivorgänge zu überwachen sind

  Nicht alle Dateivorgänge sind für jedes Protokoll gültig.

- Welche Dateifilter konfiguriert werden sollen

  Es sind nur bestimmte Kombinationen von Dateioperationen und Filtern gültig. Jedes Protokoll verfügt über einen eigenen Satz unterstützter Kombinationen.

- Gibt an, ob die Volume-Mount- und Unmount-Vorgänge überwacht werden sollen

> Es gibt eine Abhängigkeit mit drei der Parameter (`-protocol`, , `-file-operations -filters`). Die folgenden Kombinationen gelten für die drei Parameter:
>
> - Sie können die `-protocol` `-file-operations` Parameter und angeben.
> - Sie können alle drei Parameter angeben.
> - Sie können keinen Parameter angeben.

Was die FPolicy-Event-Konfiguration enthält

Sie können die folgende Liste der verfügbaren FPolicy Event-Konfigurationsparameter verwenden, um Ihre Konfiguration zu planen:

Informationstyp	Option
SVM Gibt den SVM-Namen an, den Sie mit diesem FPolicy-Ereignis verknüpfen möchten. Jede FPolicy-Konfiguration ist innerhalb einer einzelnen SVM definiert. Die externe Engine, das Richtlinienereignis, der Richtlinienumfang und die Richtlinie, die gemeinsam eine FPolicy-Konfiguration erstellen, müssen mit derselben SVM verknüpft werden.	`-vserver vserver_name`
Ereignisname Gibt den Namen an, der dem FPolicy-Ereignis zugewiesen werden soll. Wenn Sie die FPolicy erstellen, verknüpfen Sie das FPolicy Ereignis mit der Richtlinie unter Verwendung des Ereignisnamens. Der Name kann bis zu 256 Zeichen lang sein. Der Name sollte bis zu 200 Zeichen lang sein, wenn das Ereignis in einer Disaster-Recovery-Konfiguration mit MetroCluster oder SVM konfiguriert wird. Der Name kann eine beliebige Kombination der folgenden Zeichen des ASCII-Bereichs 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` Wenn Sie angeben `-protocol`, müssen Sie einen gültigen Wert im `-file-operations` Parameter angeben. Wenn sich die Protokollversion ändert, können sich die gültigen Werte ändern. Ab ONTAP 9.15.1 ermöglicht Ihnen nfsv4.0 die Erfassung von Ereignissen in NFSv4.0 und NFSv4.1.	`-protocol protocol`

Dateivorgänge Gibt die Liste der Dateivorgänge für das FPolicy-Ereignis an. Das Ereignis überprüft die in dieser Liste angegebenen Vorgänge aus allen Clientanforderungen unter Verwendung des im `-protocol` Parameter angegebenen Protokolls. Sie können ein oder mehrere Dateivorgänge mit einer durch Komma getrennten Liste auflisten. Die Liste für `-file -operations` kann einen oder mehrere der folgenden Werte enthalten: • `close` Für Dateiabgänge • `create` Für Dateierstellvorgänge • `create-dir` Für Verzeichniserstellvorgänge • `delete` Für Dateilösch-Vorgänge • `delete_dir` Für Verzeichnislösch-Vorgänge • `getattr` Für Vorgänge beim Abrufen von Attributen • `link` Für Verbindungsvorgänge • `lookup` Für Suchvorgänge • `open` Für Dateioperationen • `read` Für Dateileseingänge • `write` Für Dateischreibvorgänge • `rename` Für Dateibenennungen • `rename_dir` Für Vorgänge zum Umbenennen von Verzeichnissen • `setattr` Für Operationen zum Festlegen von Attributen • `symlink` Für symbolische Link-Vorgänge Wenn Sie angeben `-file-operations`, müssen Sie im `-protocol` Parameter ein gültiges Protokoll angeben.	`-file-operations file_operations,...`

Filter Gibt die Liste der Filter für einen bestimmten Dateivorgang für das angegebene Protokoll an. Die Werte im `-filters` Parameter werden zum Filtern von Client-Anforderungen verwendet. Die Liste kann eine oder mehrere der folgenden Elemente enthalten: Wenn Sie den `-filters` Parameter angeben, müssen Sie auch gültige Werte für die `-file-operations` `-protocol` Parameter und angeben. • `monitor-ads` Option zum Filtern der Clientanforderung nach alternativem Datenstrom. • `close-with-modification` Option zum Filtern der Clientanforderung nach Abschluss mit Änderung. • `close-without-modification` Option zum Filtern der Clientanforderung nach Schließen ohne Änderung. • `first-read` Option zum Filtern der Client-Anforderung zum ersten Lesen. • `first-write` Option zum Filtern der Client-Anforderung nach dem ersten Schreiben. • `offline-bit` Option zum Filtern der Client-Anforderung nach Offline-Bit-Satz. Wenn Sie diesen Filter festlegen, wird der FPolicy-Server nur benachrichtigt, wenn auf Offline-Dateien zugegriffen wird. • `open-with-delete-intent` Option zum Filtern der Client-Anforderung nach Öffnen mit Löschabsicht. Wenn Sie diesen Filter festlegen, wird der FPolicy-Server nur benachrichtigt, 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 wird. • `open-with-write-intent` Option zum Filtern der Client-Anfrage nach Open mit Write Intent. Die Einstellung dieses Filters führt dazu, dass der FPolicy-Server eine Benachrichtigung nur erhält, wenn versucht wird, eine Datei mit der Absicht zu öffnen, etwas darin zu schreiben. • `write-with-size-change` Option zum Filtern der Client-Anfrage nach Schreibvorgängen mit Größenänderung. • `setattr-with-owner-change` Option zum Filtern der Client-setattr-Anforderungen nach dem Ändern des Eigentümers einer Datei oder eines Verzeichnisses. • `setattr-with-group-change` Option zum Filtern der Client-setattr-Anforderungen zum Ändern der Gruppe einer Datei oder eines Verzeichnisses. `setattr-with-sacl-change` Option zum Filtern der Client-setattr-Anforderungen zum Ändern der SACL in einer Datei oder einem Verzeichnis.	`-filters filter, ...`

Ist Volumenvorgang erforderlich Gibt an, ob Monitoring für Volume-Mount- und Unmount-Vorgänge erforderlich ist. Der Standardwert ist `false`.	`-volume-operation {true`

`false}`
 	
`-filters filter, ...`
	FPolicy Zugriff verweigert Benachrichtigungen
	
	Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen für fehlgeschlagene Dateivorgänge erhalten, da sie keine Berechtigungen haben. Diese Benachrichtigungen sind wertvoll für Sicherheit, Ransomware-Schutz und Governance. Es werden Benachrichtigungen für Dateioperationen generiert, die aufgrund fehlender Berechtigungen fehlgeschlagen sind. Dazu gehören:
	
	• Fehler aufgrund von NTFS-Berechtigungen.
	• Fehler aufgrund von Unix-Modus-Bits.
	• Fehler aufgrund von NFSv4-ACLs.

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

nach Verzeichnisoperationen.

Wenn dieser Filter angegeben ist, werden die Verzeichnisvorgänge nicht überwacht.

Unterstützte Dateioperationen und Filterkombinationen ONTAP FPolicy-Monitore für SMB

Wenn Sie Ihr FPolicy-Ereignis konfigurieren, müssen Sie beachten, dass nur bestimmte Kombinationen von Dateioperationen und Filtern zur Überwachung von SMB-Dateizugriffsvorgängen unterstützt werden.

Die folgende Tabelle enthält eine Liste der unterstützten Dateivorgänge und Filterkombinationen für die FPolicy-Überwachung von SMB-Dateizugriffsereignissen:

Unterstützte Dateivorgänge	Unterstützte Filter
Schließen	Monitor-ads, Offline-Bit, Close-with-Modifizierung, Close-ohne-Änderung, Close-with-Read, Exclude-Verzeichnis
Erstellen	Monitor-ADS, Offline-Bit

Create_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Löschen	Monitor-ADS, Offline-Bit
Delete_dir	Derzeit wird kein Filter für diesen Dateivorgang 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
Umbenennen_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Sollwert	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_allokation_size_change, exclude_Directory

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen für fehlgeschlagene Dateivorgänge erhalten, da sie keine Berechtigungen haben. Die Liste der unterstützten Zugriffsverweigerung Dateioperationen und Filterkombinationen für das FPolicy Monitoring von SMB-Dateizugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützter Zugriff verweigert Dateivorgang	Unterstützte Filter
Offen	NA

Unterstützte Dateioperationen und Filterkombinationen, die ONTAP FPolicy für NFSv3 überwacht

Wenn Sie Ihr FPolicy-Ereignis konfigurieren, müssen Sie beachten, dass nur bestimmte Kombinationen von Dateioperationen und Filtern für die Überwachung von NFSv3-Dateizugriffsoperationen unterstützt werden.

Die Liste der unterstützten Dateivorgänge und Filterkombinationen für FPolicy-Überwachung von NFSv3-Dateizugriffsereignissen wird in der folgenden Tabelle aufgeführt:

Unterstützte Dateivorgänge	Unterstützte Filter

Erstellen	Offline-Bit
Create_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Löschen	Offline-Bit
Delete_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Verlinken	Offline-Bit
Suchen	Offline-Bit, exclude-dir
Lesen	Offline-Bit, First-Read
Schreiben	Offline-Bit, First-Write, Write-with-size-change
Umbenennen	Offline-Bit
Umbenennen_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Sollwert	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
Symbolischer Link	Offline-Bit

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen für fehlgeschlagene Dateivorgänge erhalten, da sie keine Berechtigungen haben. Die Liste der unterstützten Zugriffsverweigerung Dateioperationen und Filterkombinationen für das FPolicy Monitoring von NFSv3-Dateizugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützter Zugriff verweigert Dateivorgang	Unterstützte Filter
Datenzugriff	NA
Erstellen	NA
Create_dir	NA
Löschen	NA
Delete_dir	NA
Verlinken	NA

Lesen	NA
Umbenennen	NA
Umbenennen_dir	NA
Sollwert	NA
Schreiben	NA

Unterstützte Dateioperationen und Filterkombinationen, die ONTAP FPolicy für NFSv4 überwacht

Wenn Sie Ihr FPolicy-Ereignis konfigurieren, müssen Sie beachten, dass nur bestimmte Kombinationen von Dateioperationen und Filtern für die Überwachung von NFSv4-Dateizugriffsoperationen unterstützt werden.

Ab ONTAP 9.15.1 unterstützt FPolicy das NFSv4.1-Protokoll.

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

Unterstützte Dateivorgänge	Unterstützte Filter
Schließen	Offline-Bit, exclude-Directory
Erstellen	Offline-Bit
Create_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Löschen	Offline-Bit
Delete_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Getattr	Offline-Bit, exclude-Directory
Verlinken	Offline-Bit
Suchen	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
Umbenennen_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Sollwert	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
Symbolischer Link	Offline-Bit

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen für fehlgeschlagene Dateivorgänge erhalten, da sie keine Berechtigungen haben. Die folgende Tabelle enthält eine Liste der unterstützten Zugriffsverweigerung bei Dateioperationen und Filterkombinationen für die FPolicy Überwachung von NFSv4- oder NFSv4.1-Dateizugriffsereignissen:

Unterstützter Zugriff verweigert Dateivorgang	Unterstützte Filter
Datenzugriff	NA
Erstellen	NA
Create_dir	NA
Löschen	NA
Delete_dir	NA
Verlinken	NA
Offen	NA
Lesen	NA
Umbenennen	NA
Umbenennen_dir	NA
Sollwert	NA
Schreiben	NA

Vollständige Arbeitsblätter zur ONTAP FPolicy-Ereigniskonfiguration

Mit diesem Arbeitsblatt können Sie die Werte aufzeichnen, die Sie während der FPolicy-Ereigniskonfiguration benötigen. Wenn ein Parameterwert erforderlich ist, müssen Sie vor der Konfiguration des FPolicy-Ereignisses festlegen, welchen Wert für diese Parameter verwendet werden soll.

Sie sollten aufzeichnen, ob Sie die einzelnen Parametereinstellungen in die FPolicy Event-Konfiguration aufnehmen möchten, und dann den Wert für die Parameter notieren, die Sie einbeziehen möchten.

Informationstyp	Erforderlich	Einschließlich	Ihre Werte
Name der Storage Virtual Machine (SVM	Ja.	Ja.	
Ereignis-Name	Ja.	Ja.	
Protokoll	Nein		
Dateivorgänge	Nein		
Filter	Nein		
Volume-Betrieb	Nein		
Zugriff verweigert Ereignisse + (Unterstützung ab ONTAP 9.13)	Nein		

Planen Sie die FPolicy-Konfiguration

Erfahren Sie mehr über ONTAP FPolicy-Richtlinienkonfigurationen

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

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

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

Sie können auch mehrere optionale Richtlinieneinstellungen konfigurieren.

Was die FPolicy-Konfiguration enthält

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

Informationstyp	Option	Erforderlich	Standard
SVM Name Gibt den Namen der SVM an, auf der eine FPolicy erstellt werden soll.	`-vserver vserver_name`	Ja.	Keine
Name der Richtlinie Gibt den Namen der FPolicy an. Der Name kann bis zu 256 Zeichen lang sein. Wenn die Richtlinie in einer MetroCluster- oder SVM-Disaster-Recovery-Konfiguration konfiguriert ist, sollte der Name bis zu 200 Zeichen lang sein. Der Name kann eine beliebige Kombination der folgenden Zeichen des ASCII-Bereichs enthalten: • `a` Durch `z` • `A` Durch `Z` • `0` Durch `9` • „_“,„-`", and ".`“	`-policy-name policy_name`	Ja.	Keine

Ereignisnamen Gibt eine kommagetrennte Liste von Ereignissen an, die mit der FPolicy verknüpft werden sollen. • Sie können einer Richtlinie mehrere Ereignisse zuordnen. • Ein Ereignis ist spezifisch für ein Protokoll. • Sie können eine einzelne 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 mit der Richtlinie verknüpfen. • Die Ereignisse müssen bereits vorhanden sein.	`-events event_name, ...`	Ja.	Keine
Persistenter Speicher Ab ONTAP 9.14.1 gibt dieser Parameter den persistenten Speicher an, der Dateizugriffsereignisse für asynchrone, nicht obligatorische Richtlinien in der SVM erfasst.	`-persistent -store persistent_store_name`	Nein	Keine

Name der externen Engine Gibt den Namen der externen Engine an, die mit der FPolicy verknüpft werden soll. • Eine externe Engine enthält die vom Knoten benötigten Informationen zum Senden von Benachrichtigungen an einen FPolicy-Server. • Sie können FPolicy so konfigurieren, dass die native externe ONTAP Engine zum einfachen Blockieren von Dateien oder zur Verwendung einer externen Engine verwendet wird, die für die Verwendung von externen FPolicy-Servern (FPolicy-Servern) konfiguriert ist, um anspruchsvollere Datei-Blockierung und Dateimanagement zu ermöglichen. • 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, diese Richtlinie nutzt die interne ONTAP-native Engine)	`native`
Ist obligatorisches Screening erforderlich Gibt an, ob eine obligatorische Überprüfung des Dateizugriffs erforderlich ist. • Die obligatorische Screening-Einstellung legt fest, welche Maßnahmen bei einem Dateizugriff getroffen werden sollen, wenn alle primären und sekundären Server ausgefallen sind oder keine Antwort von den FPolicy-Servern innerhalb eines bestimmten Zeitlimits erhalten wird. • Wenn auf festgelegt `true`, werden Dateizugriffsereignisse verweigert. • Wenn auf festgelegt `false`, sind Dateizugriffsereignisse zulässig.	`-is-mandatory {true`	`false}`	Nein

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

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

Nein (sofern der privilegierte Zugriff nicht aktiviert ist)	Keine	*Passthrough-read* zulassen Gibt an, ob die FPolicy-Server PassThrough-Read-Services für Dateien bereitstellen können, die von den FPolicy-Servern in sekundären Speicher (Offline-Dateien) archiviert wurden: • Passthrough-read ist eine Möglichkeit, Daten von Offline-Dateien zu lesen, ohne die Daten auf den primären Speicher wiederherzustellen. Durch das Passthrough-Lesevorgang werden die Reaktionszeiten reduziert, da vor der Reaktion auf die Leseanforderung keine Dateien zurück auf den primären Storage zurückgerufen werden müssen. Zusätzlich optimiert das Passthrough-Lesevorgang die Storage-Effizienz, da es nicht mehr erforderlich ist, primären Storage mit Dateien zu belegen, die ausschließlich für Lesezugriffe abgerufen werden.	`-is-passthrough-read-enabled {true`

Anforderung für ONTAP FPolicy-Bereichskonfigurationen, wenn die FPolicy-Richtlinie die native Engine verwendet

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

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

Wenn eine FPolicy-Richtlinie, die die native Engine verwendet, für eine Freigabe oder ein Volume aktiviert `-is-file-extension-check-on-directories-enabled` ist und der Parameter `false` für die Richtlinie festgelegt ist, wird der Zugriff auf das Verzeichnis verweigert. Da die Dateierweiterungen nicht auf Verzeichnisse überprüft werden, wird bei dieser Konfiguration ein Verzeichnisvorgang verweigert, wenn er unter den Geltungsbereich der Richtlinie fällt.

Um sicherzustellen, dass der Verzeichniszugriff bei der Verwendung der nativen Engine erfolgreich `-is-file-extension-check-on-directories-enabled parameter` `true` ist, müssen Sie beim Erstellen des Gültigkeitsbereichs die auf festlegen.

Mit diesem Parameter auf `true`, Nebenstellen-Prüfungen für Verzeichnisoperationen und die Entscheidung, ob der Zugriff zu erlauben oder zu verweigern erfolgt auf der Grundlage der Erweiterungen in der FPolicy-Scope-Konfiguration enthalten oder ausgeschlossen.

- Wenn diese Option aktiviert ist, stellen die Policy-Server die Daten für die Datei über einen separaten privilegierten Datenkanal bereit, der speziell für Passdurchlesevorgänge geöffnet wurde.
- Wenn Sie Passthrough-read konfigurieren möchten, muss die Richtlinie auch so konfiguriert werden, dass ein privilegierter Zugriff möglich ist.

Vollständige ONTAP FPolicy-Richtlinienarbeitsblätter

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

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

Privilegierter Benutzername		
Ist Passthrough-read aktiviert?		

Planen der FPolicy Scope-Konfiguration

Erfahren Sie mehr über ONTAP FPolicy-Bereichskonfigurationen

Bevor Sie den FPolicy-Bereich konfigurieren, müssen Sie verstehen, was es bedeutet, einen Umfang zu erstellen. Sie müssen wissen, welche Umfang-Konfiguration enthält. Sie müssen auch verstehen, was die Anwendungsregeln von Vorrang sind. Diese Informationen können Ihnen bei der Planung der Werte helfen, die Sie festlegen möchten.

Was es bedeutet, einen FPolicy-Bereich zu erstellen

Beim Erstellen des FPolicy-Umfangs müssen die Grenzen definiert werden, für die die FPolicy gilt. Die Storage Virtual Machine (SVM) ist die grundlegende Grenze. Wenn Sie einen Bereich für eine FPolicy erstellen, müssen Sie die FPolicy definieren, für die sie gilt. Außerdem müssen Sie angeben, auf welche SVM der Umfang angewendet werden soll.

Es gibt verschiedene Parameter, die den Umfang innerhalb der angegebenen SVM weiter einschränken. Sie können den Umfang einschränken, indem Sie angeben, was im Umfang enthalten sein soll, oder indem Sie angeben, was vom Umfang ausgeschlossen werden soll. Nachdem Sie einen Bereich auf eine aktivierte Richtlinie angewendet haben, werden die Ereignisprüfungen für Richtlinien auf den durch diesen Befehl definierten Umfang 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 Scope-Konfiguration definiert die folgenden Konfigurationsinformationen:

- SVM-Name
- Name der Richtlinie
- Die Freigaben, die von dem, was überwacht wird, einbezogen oder ausgeschlossen werden sollen
- Die Exportrichtlinien, die von den überwachten Daten enthalten oder ausschließen sollen
- Die Volumes, die von den überwachten Volumes ein- oder ausgeschlossen werden sollen
- Die Dateierweiterungen, die das überwachte einschließen oder ausschließen sollen
- Ob Dateiendungsprüfungen für Verzeichnisobjekte durchgeführt werden sollen

Es gibt besondere Überlegungen für den Umfang einer Cluster FPolicy. Die Cluster-FPolicy ist eine Richtlinie, die der Cluster-Administrator für den Administrator-SVM erstellt. Wenn der Cluster-Administrator auch diesen Umfang für diese Cluster FPolicy erstellt, kann der SVM-Administrator nicht für dieselbe Richtlinie ein Angebot erstellen. Wenn der Cluster-Administrator jedoch keinen Umfang für die Cluster FPolicy erstellt, kann ein SVM-Administrator den Umfang für diese Cluster-Richtlinie erstellen. Wenn der SVM-Administrator diese Cluster-Policy erstellt, kann der Cluster-Administrator nicht anschließend Cluster-Umfang für die gleiche Cluster-Richtlinie erstellen. Dies liegt daran, dass der Cluster-Administrator den Umfang für dieselbe Cluster-Richtlinie nicht außer Kraft setzen kann.

Was sind die Anwendungsregeln von Precedence

Für die Anwendungskonfigurationen gelten die folgenden Vorrangregeln:

- Wenn eine Share in den `-shares-to-include` Parameter aufgenommen wird und das übergeordnete Volume der Share in den `-volumes-to-exclude` Parameter einbezogen wird, `-volumes-to-exclude` hat Vorrang vor `-shares-to-include`.
- Wenn eine Exportrichtlinie in den `-export-policies-to-include` Parameter eingeschlossen ist und das übergeordnete Volume der Exportrichtlinie in den `-volumes-to-exclude` Parameter eingeschlossen `-volumes-to-exclude` ist, hat Vorrang vor `-export-policies-to-include`.
- Ein Administrator kann sowohl `-file-extensions-to-include` `-file-extensions-to-exclude` Listen als auch angeben.

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

Die FPolicy Scope-Konfiguration enthält

Sie können die folgende Liste der verfügbaren FPolicy Scope-Konfigurationsparameter verwenden, um Ihre Konfiguration zu planen:

Bei der Konfiguration, welche Freigaben, Exportrichtlinien, Volumes und Dateierweiterungen ein- oder ausgeschlossen werden sollen, können die ein- und Ausschlussparameter Metacharacter wie „`?` and `*`“ enthalten. Die Verwendung von regulären Ausdrücken wird nicht unterstützt.

Informationstyp	Option
SVM Gibt den SVM-Namen an, auf dem ein FPolicy Scope erstellt werden soll. Jede FPolicy-Konfiguration ist innerhalb einer einzelnen SVM definiert. Die externe Engine, das Richtlinienereignis, der Richtlinienumfang und die Richtlinie, die gemeinsam eine FPolicy-Konfiguration erstellen, müssen mit derselben SVM verknüpft werden.	`-vserver vserver_name`

Name der Richtlinie Gibt den Namen der FPolicy an, der der Umfang angehängt werden soll. Die FPolicy muss bereits bestehen.	`-policy-name policy_name`
Zu den Aktien gehören Gibt eine durch Komma getrennte Liste von Freigaben an, die für die Policy FPolicy überwacht werden sollen, auf die der Geltungsbereich angewendet wird.	`-shares-to-include share_name, ...`
Freigaben ausschließen Gibt eine durch Komma getrennte Liste von Freigaben an, die von der Überwachung der FPolicy ausgeschlossen werden sollen, auf die der Umfang angewendet wird.	`-shares-to-exclude share_name, ...`
Volumes To include gibt eine durch Komma getrennte Liste von Volumes an, die für die Policy überwacht werden sollen, auf die der Umfang angewendet wird.	`-volumes-to-include volume_name, ...`
Volumes zum Ausschließen Gibt eine kommagetrennte Liste von Volumes an, die von der Überwachung der FPolicy ausgeschlossen werden sollen, auf die der Umfang angewendet wird.	`-volumes-to-exclude volume_name, ...`
Exportrichtlinien, die eingeschlossen werden sollen Gibt eine kommagetrennte Liste von Exportrichtlinien an, die für die FPolicy überwacht werden sollen, auf die der Umfang angewendet wird.	`-export-policies-to -include export_policy_name, ...`
Exportrichtlinien zum Ausschließen Gibt eine kommagetrennte Liste von Exportrichtlinien an, die von der Überwachung der FPolicy ausgeschlossen werden soll, auf die der Umfang angewendet wird.	`-export-policies-to -exclude export_policy_name, ...`
Zu include. Dateierweiterungen Gibt eine durch Komma getrennte Liste von Dateierweiterungen an, die für die FPolicy überwacht werden sollen, auf die der Umfang angewendet wird.	`-file-extensions-to -include file_extensions, ...`
Dateierweiterung zum Ausschließen Gibt eine durch Komma getrennte Liste von Dateierweiterungen an, die von der Überwachung der FPolicy, auf die der Umfang angewendet wird, ausgeschlossen werden sollen.	`-file-extensions-to -exclude file_extensions, ...`

Ist die Dateierweiterung für das Verzeichnis aktiviert ? Gibt an, ob die Dateinamensprüfungen auch auf Verzeichnisobjekte angewendet werden. Wenn dieser Parameter auf gesetzt `true` ist, werden die Verzeichnisobjekte den gleichen Erweiterungsprüfungen unterzogen wie normale Dateien. Wenn dieser Parameter auf eingestellt `false` ist, werden die Verzeichnisnamen nicht für Erweiterungen abgeglichen und Benachrichtigungen für Verzeichnisse gesendet, auch wenn ihre Namenserweiterungen nicht übereinstimmen. Wenn die FPolicy-Richtlinie, der der Umfang zugewiesen ist, zur Verwendung der nativen Engine konfiguriert wird, muss dieser Parameter auf festgelegt werden `true`.	`-is-file-extension -check-on-directories -enabled{true false}`

Vollständige Arbeitsblätter zum ONTAP FPolicy-Bereich

Mit diesem Arbeitsblatt können Sie die Werte aufzeichnen, die Sie während der Konfiguration des FPolicy Scope benötigen. Wenn ein Parameterwert erforderlich ist, müssen Sie vor der Konfiguration des FPolicy-Umfangs festlegen, welchen Wert für diese Parameter verwendet werden soll.

Sie sollten aufzeichnen, ob die einzelnen Parameter in die FPolicy Scope-Konfiguration einbezogen werden sollen, und dann den Wert für die Parameter notieren, die Sie einbeziehen möchten.

Informationstyp	Erforderlich	Einschließlich	Ihre Werte
Name der Storage Virtual Machine (SVM	Ja.	Ja.	
Name der Richtlinie	Ja.	Ja.	
Einzuschließen von Freigaben	Nein		
Auszuschließende Freigaben	Nein		
Volumes die einbezogen werden sollen	Nein		
Auszuschließende Volumes	Nein		
Richtlinien exportieren, die einbezogen werden sollen	Nein		
Auszuschließende Richtlinien exportieren	Nein		
Einzuschließen von Dateierweiterungen	Nein		
Auszuschließende Dateierweiterung	Nein		

Ist die Dateierweiterung für das Verzeichnis aktiviert?	Nein		