FPolicy ermöglicht Datei-Monitoring und -Management auf SVMs

ONTAP 9

NetApp
September 12, 2024

Inhalt

FPolicy ermöglicht Datei-Monitoring und -Management auf SVMs 1
FPolicy verstehen 1
Planen der FPolicy-Konfiguration 10
Erstellen Sie die FPolicy-Konfiguration 49
Managen von FPolicy-Konfigurationen 57

FPolicy ermöglicht Datei-Monitoring und -Management auf SVMs

FPolicy verstehen

Was die beiden Teile der FPolicy Lösung sind

FPolicy ist ein Benachrichtigungs-Framework für den Dateizugriff, mit dem Ereignisse für den Dateizugriff auf Storage Virtual Machines (SVMs) über Partnerlösungen überwacht und gemanagt werden können. Partnerlösungen unterstützen Sie bei der Bewältigung verschiedener Anwendungsfälle wie Daten-Governance und Compliance, Ransomware-Schutz und Datenmobilität.

Bei den Partnerlösungen zählen sowohl von NetApp unterstützte Lösungen von Drittanbietern als auch NetApp Produkte Workload Security und Cloud Data Sense.

Es gibt zwei Teile zu einer FPolicy Lösung. Das ONTAP FPolicy Framework verwaltet Aktivitäten im Cluster und sendet Benachrichtigungen an die Partnerapplikation (auch externe FPolicy Server genannt). Externe FPolicy Server verarbeiten Benachrichtigungen, die von ONTAP FPolicy gesendet werden, um Kundennutzungsfälle zu erfüllen.

Das ONTAP Framework erstellt und pflegt die FPolicy Konfiguration, überwacht Dateiereignisse und sendet Benachrichtigungen an externe FPolicy Server. ONTAP FPolicy bietet die Infrastruktur für die Kommunikation zwischen externen FPolicy Servern und Storage Virtual Machine (SVM) Nodes.

Das FPolicy-Framework stellt eine Verbindung zu externen FPolicy-Servern her und sendet Benachrichtigungen für bestimmte Dateisystemereignisse an die FPolicy-Server, wenn diese Ereignisse als Folge des Client-Zugriffs auftreten. Die externen FPolicy Server verarbeiten die Benachrichtigungen und senden Antworten zurück auf den Knoten. Was als Folge der Benachrichtigungsverarbeitung geschieht, hängt von der Anwendung ab und ob die Kommunikation zwischen Knoten und externen Servern asynchron oder synchron ist.

Was sind synchrone und asynchrone 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 von Benachrichtigungen an FPolicy-Server tut.

- **Asynchronous Notifications**

  Bei asynchronen Benachrichtigungen wartet der Node nicht auf eine Antwort des FPolicy Servers, wodurch der Gesamtdurchsatz des Systems verbessert wird. Diese Art der Benachrichtigung ist für Anwendungen geeignet, bei denen der FPolicy-Server aufgrund der Benachrichtigungsbewertung keine Maßnahmen erfordert. Asynchrone Benachrichtigungen kommen beispielsweise zum Einsatz, wenn der SVM-Administrator (Storage Virtual Machine) den Dateizugriff überwachen und prüfen möchte.

  Wenn bei einem FPolicy-Server im asynchronen Modus ein Netzwerkausfall auftritt, werden FPolicy Benachrichtigungen, die während des Ausfalls generiert wurden, auf dem Storage-Node gespeichert. Wenn der FPolicy-Server wieder online geschaltet wird, wird er über die gespeicherten Benachrichtigungen

benachrichtigt und kann sie vom Speicher-Node abrufen. Die Länge der Speicherung der Benachrichtigungen während eines Ausfalls kann so bis zu 10 Minuten betragen.

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.

- **Synchrone Benachrichtigungen**

  Wenn der FPolicy-Server für die Ausführung im synchronen Modus konfiguriert ist, muss er jede Benachrichtigung bestätigen, bevor der Clientvorgang fortgesetzt werden kann. Diese Art der Benachrichtigung wird verwendet, wenn eine Aktion erforderlich ist, basierend auf den Ergebnissen der Auswertung der Benachrichtigung. Synchrone Benachrichtigungen werden beispielsweise verwendet, wenn der SVM-Administrator Anfragen basierend auf den auf dem externen FPolicy-Server festgelegten Kriterien zulassen oder ablehnen möchte.

Synchrone und asynchrone Applikationen

Es gibt viele mögliche Einsatzmöglichkeiten für FPolicy-Applikationen, sowohl asynchron als auch synchron.

Asynchrone Applikationen sind solche, bei denen der externe FPolicy-Server den Zugriff auf Dateien oder Verzeichnisse nicht verändert oder Daten auf der Storage Virtual Machine (SVM) verändert. Beispiel:

- Dateizugriff und Revisionsprotokollierung
- Storage-Ressourcenmanagement

Synchrone Applikationen sind solche, bei denen der Datenzugriff geändert wird oder die Daten vom externen FPolicy-Server geändert werden. Beispiel:

- Kontingentverwaltung
- Blockierung des Dateizugriffs
- Dateiarchivierung und hierarchisches Storage-Management
- Verschlüsselungs- und Entschlüsselungsdienste
- Komprimierungs- und Dekomprimierungsservices

FPolicy persistente Speicher

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

Diese Funktion ist nur im externen FPolicy-Modus verfügbar. Die Partneranwendung, die Sie verwenden, muss diese Funktion unterstützen. Stellen Sie sicher, dass diese FPolicy-Konfiguration von Ihrem Partner unterstützt wird.

Ab ONTAP 9.15.1 wird die Konfiguration persistenter FPolicy-Speicher vereinfacht. Der `persistent-store`

`create` Der Befehl automatisiert die Volume-Erstellung für die SVM und konfiguriert das Volume mit Best Practices für persistenten Speicher.

Weitere Informationen zu Best Practices für persistenten Speicher finden Sie unter "Anforderungen, Überlegungen und Best Practices für die Konfiguration von FPolicy".

Informationen zum Hinzufügen persistenter Speicher finden Sie unter "Erstellen persistenter Speicher".

FPolicy-Konfigurationstypen

Es gibt zwei grundlegende FPolicy-Konfigurationstypen. Eine Konfiguration verwendet externe FPolicy Server zur Verarbeitung und Bearbeitung von Benachrichtigungen. Die andere Konfiguration verwendet keine externen FPolicy Server; stattdessen verwendet es den internen, nativen FPolicy Server von ONTAP für einfaches File Blocking auf Basis von Erweiterungen.

- **Konfiguration des externen FPolicy Servers**

  Die Benachrichtigung wird an den FPolicy-Server gesendet, der die Anforderung einliest und Regeln anwendet, um zu bestimmen, ob der Knoten den angeforderten Dateibetrieb zulassen soll. Für synchrone Richtlinien sendet der FPolicy-Server dann eine Antwort an den Node, um die angeforderte Dateioperation zu ermöglichen oder zu blockieren.

- **Native FPolicy Server-Konfiguration**

  Die Benachrichtigung wird intern gescreent. Die Anforderung wird zulässig oder abgelehnt, basierend auf den im FPolicy-Umfang konfigurierten Dateiendungeinstellungen.

  Hinweis: Nicht ablehnte Dateiendungsanfragen werden protokolliert.

Wann eine native FPolicy Konfiguration erstellt werden soll

Native FPolicy-Konfigurationen verwenden die interne ONTAP FPolicy Engine, um Dateivorgänge basierend auf der Dateierweiterung zu überwachen und zu blockieren. Diese Lösung erfordert keine externen FPolicy Server (FPolicy Server). Wenn diese einfache Lösung benötigt wird, ist die Verwendung einer nativen File Blocking-Konfiguration angemessen.

Das native File Blocking ermöglicht Ihnen die Überwachung aller Dateivorgänge, die mit konfigurierten Vorgängen und Filterereignissen übereinstimmen, und verweigert dann den Zugriff auf Dateien mit bestimmten Erweiterungen. Dies ist die Standardkonfiguration.

Mit dieser Konfiguration wird der Dateizugriff nur auf Basis der Dateiendung blockiert. Beispielsweise zum Blockieren von Dateien, die enthalten `mp3` Erweiterungen: Sie konfigurieren eine Richtlinie, um Benachrichtigungen für bestimmte Vorgänge mit Zieldateierweiterungen von bereitzustellen `mp3`. Die Richtlinie ist so konfiguriert, dass sie verweigert wird `mp3` Dateianforderungen für Vorgänge, die Benachrichtigungen generieren

Das gilt für native FPolicy-Konfigurationen:

- Dieselben Filter und Protokolle, die von FPolicy Server-basierten Dateiscreening unterstützt werden, werden auch für das native File Blocking unterstützt.
- Native File Blocking- und FPolicy-basierte Datei-Screening-Applikationen können gleichzeitig konfiguriert werden.

Dazu können Sie zwei separate FPolicy Richtlinien für die Storage Virtual Machine (SVM) konfigurieren, wobei eine für natives File Blocking konfiguriert ist und eine für FPolicy-Server-basierte Datei-Screening konfiguriert ist.

- Die native File Blocking-Funktion nur Bildschirme Dateien auf der Grundlage der Erweiterungen und nicht auf den Inhalt der Datei.
- Bei symbolischen Links verwendet das native File Blocking die Dateiendung der Root-Datei.

Weitere Informationen zu "FPolicy: Native Dateisperrung".

Wenn eine Konfiguration erstellt werden soll, die externe FPolicy-Server verwendet

FPolicy-Konfigurationen, die für die Verarbeitung und das Management von Benachrichtigungen über externe FPolicy-Server verfügen, bieten zuverlässige Lösungen für Anwendungsfälle, in denen mehr als einfaches File Blocking auf Basis einer Dateierweiterung erforderlich ist.

Sie sollten eine Konfiguration erstellen, die externe FPolicy-Server verwendet, wenn Sie solche Dinge wie Überwachung und Aufzeichnung von Dateizugriffsereignissen, Bereitstellung von Quotendiensten, Durchführung von Dateiblockierung auf der Grundlage von Kriterien andere als einfache Dateierweiterungen, Bereitstellung von Datenmigrationsservices unter Verwendung von hierarchischen Speichermanagement-Anwendungen, Alternativ können Sie feingranulare Richtlinien anbieten, die nur eine Teilmenge an Daten in der Storage Virtual Machine (SVM) überwachen.

Rollen, die Cluster-Komponenten bei FPolicy Implementierung spielen

In einer FPolicy Implementierung spielen der Cluster, die enthaltenen Storage Virtual Machines (SVMs) und Daten-LIFs eine Rolle.

- * Cluster*

  Das Cluster enthält das FPolicy Management-Framework und verwaltet Informationen zu allen FPolicy-Konfigurationen im Cluster.

- **SVM**

  Eine FPolicy-Konfiguration wird auf SVM-Ebene definiert. Der Konfigurationsumfang ist die SVM, die nur auf SVM-Ressourcen ausgeführt wird. Eine SVM-Konfiguration kann keine Benachrichtigungen für Dateizugriffsanfragen überwachen und senden, die sich auf Daten auf einer anderen SVM befinden.

  FPolicy-Konfigurationen können auf der Admin-SVM definiert werden. Nachdem die Konfigurationen auf der Administrator-SVM definiert wurden, können sie in allen SVMs angezeigt und verwendet werden.

- **Daten-LIFs**

  Verbindungen zu den FPolicy-Servern werden über Daten-LIFs, die zur SVM mit der FPolicy-Konfiguration gehören, hergestellt. Die für diese Verbindungen verwendeten Daten-LIFs können ein Failover auf dieselbe Weise durchführen wie die Daten-LIFs für den normalen Client-Zugriff.

Wie FPolicy mit externen FPolicy-Servern funktioniert

Nachdem FPolicy auf der Storage Virtual Machine (SVM) konfiguriert und aktiviert wurde, wird FPolicy auf jedem Node ausgeführt, an dem die SVM teilnimmt. FPolicy ist für die

Einrichtung und Wartung von Verbindungen mit externen FPolicy-Servern (FPolicy-Servern), für die Benachrichtigungsverarbeitung und das Management von Benachrichtigungsmeldungen zu und von FPolicy-Servern verantwortlich.

Darüber hinaus hat FPolicy im Rahmen des Verbindungsmanagements folgende Aufgaben:

- Stellt sicher, dass die Dateibenachrichtigung durch die richtige LIF an den FPolicy-Server fließt.
- Stellt sicher, dass beim Senden von Benachrichtigungen an die FPolicy-Server ein Lastausgleich erfolgt, wenn mehrere FPolicy-Server mit einer Richtlinie verknüpft sind.
- Versucht, die Verbindung wiederherzustellen, wenn eine Verbindung zu einem FPolicy-Server unterbrochen wird.
- Sendet Benachrichtigungen über eine authentifizierte Sitzung an FPolicy Server.
- Verwaltet die vom FPolicy-Server für die Verarbeitung von Clientanforderungen festgelegte Passthrough-Datenverbindung, wenn das Passthrough-Lesevorgang aktiviert ist.

Wie Kontrollkanäle für die FPolicy Kommunikation verwendet werden

FPolicy initiiert eine Steuerkanalverbindung zu einem externen FPolicy Server von den Daten-LIFs jedes Nodes, der an einer Storage Virtual Machine (SVM) beteiligt ist. FPolicy verwendet Kontrollkanäle für die Übertragung von Dateibenachrichtigungen. Daher können bei einem FPolicy-Server je nach SVM-Topologie mehrere Kontrollkanalverbindungen zu erkennen sein.

Verwendung von privilegierten Datenzugriffskanälen für die synchrone Kommunikation

Bei synchronen Anwendungsfällen greift der FPolicy Server über einen privilegierten Datenpfad auf die auf der Storage Virtual Machine (SVM) befindlichen Daten zu. Der Zugriff über den privilegierten Pfad stellt dem FPolicy-Server das komplette Dateisystem zur Verfügung. Es 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 vom Root der SVM auf das gesamte Filesystem zugreifen kann, muss die Verbindung mit dem privilegierten Datenkanal sicher sein.

Verwendung von FPolicy Connection Anmeldeinformationen mit privilegierten Datenzugriffskanälen

Der FPolicy-Server stellt privilegierte Datenzugangsverbindungen zu Cluster-Knoten mithilfe einer bestimmten Windows-Benutzeranmeldeinformationen bereit, die mit der FPolicy-Konfiguration gespeichert werden. SMB ist das einzige unterstützte Protokoll für eine Verbindung mit einem privilegierten Channel für den Datenzugriff.

Wenn der FPolicy-Server einen privilegierten Datenzugriff erfordert, müssen die folgenden Bedingungen erfüllt sein:

- Eine SMB-Lizenz muss auf dem Cluster aktiviert sein.
- Der FPolicy-Server muss unter den in der FPolicy-Konfiguration konfigurierten Anmeldeinformationen ausgeführt werden.

Beim Herstellen einer Datenkanalverbindung verwendet FPolicy die Anmeldeinformationen für den angegebenen Windows-Benutzernamen. Der Datenzugriff erfolgt über den Admin-Anteil „ONTAP_ADMIN“.

Was die Gewährung von Super-User-Anmeldeinformationen für privilegierten Datenzugriff bedeutet

ONTAP verwendet die Kombination aus der IP-Adresse und den in der FPolicy-Konfiguration konfigurierten Benutzerberechtigungen, um dem FPolicy-Server Super-Benutzeranmeldeinformationen zu erteilen.

Der Superuser-Status gewährt die folgenden Berechtigungen, wenn der FPolicy-Server auf Daten zugreift:

- Vermeiden Sie Berechtigungsprüfungen

  Der Benutzer vermeidet Überprüfungen von Dateien und Verzeichniszugriff.

- Besondere Sperrrechte

  ONTAP ermöglicht Lese-, Schreib- oder Änderungszugriff auf beliebige Dateien, unabhängig von vorhandenen Sperren. Wenn der FPolicy-Server Byte-Sperren auf der Datei nimmt, werden bestehende Sperren auf der Datei sofort entfernt.

- Umgehen Sie alle FPolicy-Prüfungen

  Der Zugriff generiert keine FPolicy-Benachrichtigungen.

So managt FPolicy die Richtlinienverarbeitung

Ihrer Storage Virtual Machine (SVM) können mehrere FPolicy Richtlinien zugewiesen sein, von denen jede eine andere Priorität hat. Um eine entsprechende FPolicy-Konfiguration auf der SVM zu erstellen, ist es wichtig zu verstehen, wie FPolicy die Richtlinienverarbeitung managt.

Jede Dateizugriffsanforderung wird zunächst ausgewertet, um festzustellen, welche Richtlinien dieses Ereignis überwachen. Wenn es sich um ein überwachtes Ereignis handelt, werden Informationen über das überwachte Ereignis zusammen mit interessierten Richtlinien an FPolicy weitergeleitet, wo es ausgewertet wird. Jede Richtlinie wird in der Reihenfolge der zugewiesenen Priorität bewertet.

Beim Konfigurieren von Richtlinien sollten Sie die folgenden Empfehlungen berücksichtigen:

- Wenn eine Richtlinie immer vor anderen Richtlinien bewertet werden soll, konfigurieren Sie diese Richtlinie mit höherer Priorität.
- Wenn der Erfolg des angeforderten Dateizugriffs bei einem überwachten Ereignis eine Voraussetzung für eine Dateianforderung ist, die anhand einer anderen Richtlinie ausgewertet wird, geben Sie der Richtlinie, die den Erfolg oder den Fehler des ersten Dateivorgangs steuert, eine höhere Priorität.

  Wenn eine Richtlinie beispielsweise Funktionen zur Dateiarchivierung und -Wiederherstellung auf FPolicy managt und eine zweite Richtlinie Dateizugriffsvorgänge in der Online-Datei managt, Die Richtlinie für die Wiederherstellung von Dateien muss eine höhere Priorität haben, damit die Datei wiederhergestellt wird, bevor der Vorgang, der von der zweiten Richtlinie gemanagt wird, zulässig ist.

- Wenn Sie möchten, dass alle Richtlinien, die für einen Dateizugriffsvorgang gelten, ausgewertet werden, sollten Sie synchrone Richtlinien mit niedrigerer Priorität betrachten.

Sie können Richtlinienprioritäten für vorhandene Richtlinien neu anordnen, indem Sie die Nummer der Richtliniensequenz ändern. Um Richtlinien basierend auf der geänderten Prioritätsreihenfolge jedoch FPolicy bewerten zu können, müssen Sie die Richtlinie mit der geänderten Sequenznummer deaktivieren und erneut aktivieren.

Was ist der Kommunikationsprozess zwischen Knoten und externem FPolicy-Server

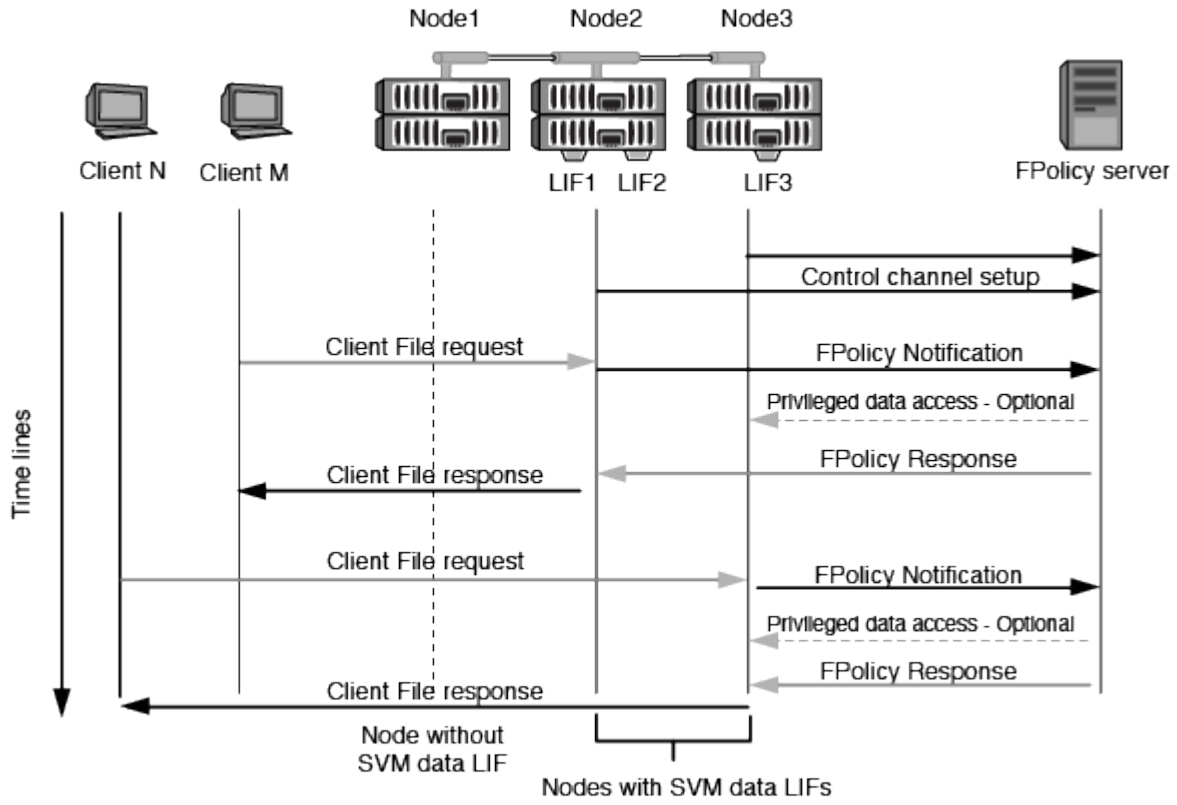
Um Ihre FPolicy-Konfiguration richtig zu planen, sollten Sie verstehen, was der Knoten-zu-externe FPolicy Server-Kommunikationsprozess ist.

Jeder Node, der an jeder Storage Virtual Machine (SVM) teilnimmt, initiiert mithilfe von TCP/IP eine Verbindung zu einem externen FPolicy Server (FPolicy Server). Verbindungen zu den FPolicy-Servern werden mithilfe von Node-Daten-LIFs eingerichtet. Daher kann ein teilnehmender Node eine Verbindung nur einrichten, wenn der Node über eine funktionsfähige Daten-LIF für die SVM verfügt.

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

Die Verbindung stellt von jedem der Nodes, die an jeder SVM teilnehmen, über die Daten-LIF einen Kontrollkanal zum FPolicy-Server bereit. Wenn IPv4- und IPv6-Daten-LIF-Adressen auf demselben teilnehmenden Node vorhanden sind, versucht FPolicy zudem, Verbindungen sowohl für IPv4 als auch für IPv6 herzustellen. Daher muss der FPolicy-Server in einem Szenario, in dem die SVM über mehrere Nodes erweitert wird oder wenn sowohl IPv4- als auch IPv6-Adressen vorhanden sind, bereit sein, nach Aktivierung der FPolicy auf der SVM mehrere Kontrollkanaleinrichtungsanfragen vom Cluster aus zu bearbeiten.

Wenn beispielsweise ein Cluster drei Nodes hat —-Node1, Node2 und Node3- und SVM-Daten-LIFs werden über nur Node2 und Node3 verteilt – werden die Kontrollkanäle nur von Node2 und Node3 aus initiiert, unabhängig von der Verteilung der Daten-Volumes. Sagen wir, dass Node2 zwei Daten-LIFs hat --LIF1 und LIF2 — die zur SVM gehören und dass die anfängliche Verbindung von LIF1 ist. Wenn LIF1 fehlschlägt, versucht FPolicy, einen Kontrollkanal von LIF2 einzurichten.



So managt FPolicy die externe Kommunikation während LIF-Migration oder Failover

Daten-LIFs können zu Daten-Ports im selben Node oder zu Daten-Ports eines Remote Nodes migriert werden.

Bei einem Failover oder der Migration einer Daten-LIF wird eine neue Kontrollkanal-Verbindung zum FPolicy-Server hergestellt. FPolicy kann dann erneut versuchen SMB- und NFS-Client-Anforderungen zu versuchen, die abgelaufen sind. Mit dem Ergebnis, dass neue Benachrichtigungen an die externen FPolicy-Server

gesendet werden. Der Node lehnt FPolicy-Serverantworten an ursprüngliche, zeitlich begrenzte SMB- und NFS-Anforderungen ab.

Wie FPolicy die externe Kommunikation beim Node Failover managt

Wenn der Cluster-Node, der die für die FPolicy Kommunikation verwendeten Daten-Ports hostet, ausfällt, bricht ONTAP die Verbindung zwischen dem FPolicy-Server und dem Node aus.

Die Auswirkungen eines Cluster Failover auf den FPolicy-Server können durch Konfiguration der Failover-Richtlinie reduziert werden, um den in der FPolicy-Kommunikation verwendeten Daten-Port zu einem anderen aktiven Node zu migrieren. Nach Abschluss der Migration wird über den neuen Daten-Port eine neue Verbindung hergestellt.

Wenn die Failover-Richtlinie nicht für die Migration des Daten-Ports konfiguriert ist, muss der FPolicy-Server warten, bis der ausgefallene Node angezeigt wird. Nachdem der Knoten aktiv ist, wird eine neue Verbindung von diesem Knoten mit einer neuen Session-ID initiiert.

> Der FPolicy-Server erkennt unterbrochene Verbindungen mit der Keep-Alive-Protokollnachricht. Bei der Konfiguration von FPolicy wird die Zeitüberschreitung für das Löschen der Sitzungs-ID festgelegt. Die standardmäßige Keep-Alive-Zeitüberschreitung beträgt zwei Minuten.

So funktionieren FPolicy Services über SVM-Namespaces hinweg

ONTAP stellt einen Namespace für Unified Storage Virtual Machine (SVM) bereit. Volumes im Cluster werden gemeinsam mit Verbindungen zu einem einzigen logischen File-System verbunden. Der FPolicy-Server erkennt die Namespace-Topologie und bietet FPolicy Services für den gesamten Namespace.

Der Namespace ist spezifisch und in der SVM enthalten. Daher wird der Namespace nur aus dem SVM-Kontext angezeigt. Namespaces haben die folgenden Eigenschaften:

- In jeder SVM ist ein einziger Namespace vorhanden, wobei der Root-Namespace das Root-Volume ist und im Namespace als „Schrägstrich“ (/) dargestellt ist.
- Alle anderen Volumes verfügen über Verbindungspunkte unter dem Root (/).
- Volume-Verbindungen sind für Clients transparent.
- Ein einzelner NFS-Export kann Zugriff auf den vollständigen Namespace bieten. Andernfalls können Exportrichtlinien bestimmte Volumes exportieren.
- SMB-Shares können auf dem Volume oder qtrees innerhalb des Volume oder in jedem Verzeichnis im Namespace erstellt werden.
- Die Namespace-Architektur ist flexibel.

  Beispiele für typische Namespace-Architekturen:

  - Ein Namespace mit einem einzelnen Zweig aus dem Root
  - Ein Namespace mit mehreren Zweigen vom Root
  - Ein Namespace mit mehreren nicht verzweigten Volumes vom Root

FPolicy Passthrough-Read verbessert die Benutzerfreundlichkeit für hierarchisches Storage-Management

PassThrough-Read ermöglicht es dem FPolicy Server (funktioniert als hierarchischer Storage Management (HSM) Server) Lesezugriff auf Offline-Dateien zu bieten, ohne die Datei vom sekundären Storage-System auf das primäre Storage-System zurückrufen zu müssen.

Wenn ein FPolicy Server so konfiguriert wird, dass HSM für Dateien auf einem SMB-Server bereitgestellt wird, erfolgt eine richtlinienbasierte Dateimigration, bei der die Dateien offline auf dem Sekundärspeicher gespeichert werden, während nur eine Stub-Datei im Primärspeicher bleibt. Obwohl eine Stub-Datei für Clients als normale Datei erscheint, handelt es sich eigentlich um eine spärliche Datei, die die gleiche Größe der ursprünglichen Datei hat. In der spärlichen Datei ist das SMB-Offline-Bit gesetzt und verweist auf die eigentliche Datei, die zum sekundären Storage migriert wurde.

Wenn eine Leseanfrage für eine Offline-Datei eingeht, muss der angeforderte Inhalt in der Regel zurück im primären Storage abgerufen werden. Der Zugriff erfolgt dann über den Primär-Storage. Der Rückruf von Daten auf den primären Storage hat mehrere unerwünschte Auswirkungen. Zu den unerwünschten Auswirkungen gehört die höhere Latenz bei Client-Anfragen, die durch das Abrufen des Inhalts vor der Reaktion auf die Anforderung verursacht werden, und der höhere Verbrauch an Speicherplatz, der für abgerufene Dateien im primären Storage benötigt wird.

FPolicy Passthrough-read ermöglicht dem HSM-Server (der FPolicy Server) einen Lesezugriff auf migrierte Offline-Dateien, ohne die Datei vom sekundären Storage-System auf das primäre Storage-System zurückrufen zu müssen. Statt die Dateien zurück auf den Primär-Storage zu zurückrufen, können Leseanforderungen direkt aus dem Sekundärspeicher abgerufen werden.

Copy Offload (ODX) wird bei FPolicy-Passthrough-Vorgang nicht unterstützt.

Passthrough-read verbessert die Benutzerfreundlichkeit durch die folgenden Vorteile:

- Lesezugriffe können auch dann bedient werden, wenn der primäre Storage nicht über genügend Speicherplatz verfügt, um die angeforderten Daten zurück auf den primären Storage abzurufen.
- Besseres Kapazitäts- und Performance-Management, wenn eine Zunahme des Datenaufrufs auftreten kann, beispielsweise wenn ein Skript oder eine Backup-Lösung auf viele Offline-Dateien zugreifen muss.
- Leseanforderungen für Offline-Dateien in Snapshot Kopien können verarbeitet werden.

  Da Snapshot-Kopien nur leseverwendet werden, kann der FPolicy Server die ursprüngliche Datei nicht wiederherstellen, wenn die Stub-Datei in einer Snapshot-Kopie befindet. Dieses Problem wird durch die Verwendung von Passthrough-Read behoben.

- Richtlinien können eingerichtet werden, die steuern, wenn Leseanforderungen über den Zugriff auf die Datei im sekundären Storage verarbeitet werden und wann die Offline-Datei an den primären Storage abgerufen werden soll.

  Beispielsweise kann eine Richtlinie auf dem HSM-Server erstellt werden, die die Anzahl der Zugriffszeiten für die Offline-Datei in einem bestimmten Zeitraum angibt, bis die Datei zurück zum primären Storage migriert wurde. Diese Art von Richtlinie verhindert das Abrufen von Dateien, auf die selten zugegriffen wird.

Wie Leseanforderungen gemanagt werden, wenn FPolicy Passthrough-read aktiviert ist

Sie sollten verstehen, wie Leseanforderungen gemanagt werden, wenn FPolicy Passthrough-Read aktiviert ist,

damit Sie die Konnektivität zwischen der Storage Virtual Machine (SVM) und den FPolicy Servern optimal konfigurieren können.

Wenn FPolicy Passthrough-Read aktiviert ist und die SVM eine Anfrage für eine Offline-Datei erhält, sendet FPolicy über den Standard-Verbindungskanal eine Benachrichtigung an den FPolicy-Server (HSM-Server).

Nach Erhalt der Benachrichtigung liest der FPolicy-Server die Daten aus dem in der Benachrichtigung gesendeten Dateipfad und sendet die angeforderten Daten über die Verbindung mit privilegierten Lesevorgängen mit Passthrough-Lesevorgängen, die zwischen der SVM und dem FPolicy-Server hergestellt wurde.

Nach dem Senden der Daten reagiert der FPolicy-Server dann auf die Leseanforderung als ZULASSEN oder ABLEHNEN. Basierend darauf, ob die Leseanforderung zulässig oder verweigert wird, sendet ONTAP entweder die angeforderten Informationen oder sendet eine Fehlermeldung an den Client.

Planen der FPolicy-Konfiguration

Anforderungen, Überlegungen und Best Practices für die Konfiguration von 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 für die Kommunikation mit den FPolicy-Servern verwendet werden, müssen konfiguriert werden `cifs` Als eines der zulässigen Protokolle.

  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, das `autosize-mode` Parameter können dem Volume als Antwort auf die Menge des genutzten Speicherplatzes helfen.

    - ONTAP 9.14.1: Die `size` Der Parameter wird während der Volume-Erstellung für ein maximales Limit konfiguriert.
- Setzen Sie die Snapshot-Richtlinie auf `none` Für das persistente Speicher-Volume anstelle von `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` Der Parameter wird während der Erstellung eines persistenten Speichers automatisch auf „none“ konfiguriert.
    - ONTAP 9.14.1: Die `snapshot-policy` Parameter ist auf konfiguriert `none` Während der Volume-Erstellung:
- 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 Speicher-Volume von einem Node zu einem anderen in derselben SVM verschoben wird, werden die noch zu verarbeitenden Benachrichtigungen auch in den neuen Node verschoben. Sie müssen das erneut ausführen `fpolicy persistent-store create` Befehl auf einem der Knoten nach dem Verschieben des Volumes, um sicherzustellen, dass die ausstehenden Benachrichtigungen an den externen Server gesendet werden.

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 ist auf festgelegt `true`, Verzeichnis-Objekte werden den gleichen Erweiterungen Prüfungen wie normale Dateien unterzogen.

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 auszuführen `statistics show –object workload` Befehl zum Anzeigen von Workload-Statistiken. 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`*

   Der `fpolicy` Und `fpolicy_server` Zähler bieten Informationen zu verschiedenen Leistungsparametern, die in der folgenden Tabelle beschrieben werden.

Zähler	Beschreibung
• „fpolicy“-Zähler*	Abgebrochene_Anforderungen

Zähler	Beschreibung
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
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	• Zähler „fpolicy_Server“*
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

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.

Was sind die Schritte zum Einrichten einer FPolicy Konfiguration

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 verwenden `protobuf` Motorformat. Wenn eingestellt auf `protobuf`, Die Benachrichtigungen werden in binärer Form mit Google protobuf codiert. Bevor Sie das Motorformat auf einstellen `protobuf`, Stellen Sie sicher, dass der FPolicy-Server auch unterstützt `protobuf` Deserialisierung. 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 ist die Einrichtung mit FPolicy möglich "Persistente Speicher" So erfassen Sie Dateizugriffsereignisse für asynchrone, nicht obligatorische Richtlinien in der SVM: 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` Der 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 Konfiguration der externen FPolicy Engine

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
- Ob das Motorformat ist `xml` Oder `protobuf`

  Ab ONTAP 9.15.1 können Sie das verwenden `protobuf` Motorformat. Wenn eingestellt auf `protobuf`, Die Benachrichtigungen werden in binärer Form mit Google protobuf codiert. Bevor Sie das Motorformat auf einstellen `protobuf`, Stellen Sie sicher, dass der FPolicy-Server auch unterstützt `protobuf` Deserialisierung.

  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 aus `protobuf` Bis `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.

Der `vserver fpolicy policy external-engine create` Mit dem Befehl wird eine FPolicy externe 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` Bis `z` • `A` Bis `Z` • `0` Bis `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 eingestellt auf `synchronous`, Die Verarbeitung von Dateianfragen sendet eine Benachrichtigung an den FPolicy-Server, wird aber dann erst fortgesetzt, nachdem eine Antwort vom FPolicy-Server erhalten 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 eingestellt auf `asynchronous`, Die Verarbeitung von Dateianfragen sendet 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 Werte 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 eingestellt auf `no-auth`, Keine Authentifizierung erfolgt. Die Kommunikationsverbindung wird über TCP hergestellt. • Wenn eingestellt auf `server-auth`, Die SVM authentifiziert den FPolicy-Server mithilfe einer SSL-Server-Authentifizierung. • Wenn eingestellt auf `mutual-auth`. Gegenseitige Authentifizierung erfolgt zwischen der SVM und dem FPolicy-Server. Die SVM authentifiziert den FPolicy-Server und der FPolicy-Server authentifiziert die SVM. Wenn Sie die gegenseitige SSL-Authentifizierung konfigurieren, müssen Sie auch die konfigurieren `-certificate-common-name`, `-certificate-serial`, und `-certifcate-ca` Parameter.	`-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 angeben `mutual-auth` Für das `-ssl-option` Parameter. Sie müssen einen Wert für das angeben `-certificate-common-name` Parameter.	`-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 angeben `mutual-auth` Für das `-ssl-option` Parameter. Sie müssen einen Wert für das angeben `-certificate-serial` Parameter.	`-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 angeben `mutual-auth` Für das `-ssl-option` Parameter. Sie müssen einen Wert für das angeben `-certificate-ca` Parameter.	`-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 Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Dass 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 ist `0`, Die Option ist deaktiviert und Cancel Request Nachrichten werden nicht an den FPolicy-Server gesendet. Die Standardeinstellung lautet `20s`.	`-reqs-cancel-timeout` `integer`[H m m m V natürlich]
Timeout für Abbruch einer Anfrage Gibt die Zeitüberschreitung in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Zum Abbruch einer Anfrage. Der Bereich für diesen Wert ist `0` Bis `200`.	`-reqs-abort-timeout` ` `integer`[H m m m V natürlich]

Intervall für das Senden von Statusanforderungen Gibt das Intervall in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Nach dem eine Statusanforderung an den FPolicy-Server gesendet wird. Der Bereich für diesen Wert ist `0` Bis `50`. Wenn der Wert auf festgelegt ist `0`, Die Option ist deaktiviert und Status Request Nachrichten werden nicht an den FPolicy-Server gesendet. Die Standardeinstellung lautet `10s`.	`-status-req-interval integer`[H m m m V natürlich]
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`. Die Standardeinstellung lautet `500`.	`-max-server-reqs integer`
Timeout zum Trennen eines nicht ansprechenden FPolicy Servers Gibt das Zeitintervall in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Nach der 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. Es gibt entweder eine maximal zulässige Anzahl von Anforderungen `50` (Die Standardeinstellung) oder die vom angegebene Zahl `max-server-reqs-` Parameter. Der Bereich für diesen Wert ist `1` Bis `100`. Die Standardeinstellung lautet `60s`.	`-server-progress -timeout integer`[H m m m V natürlich]
Intervall zum Senden von Keep-Alive-Nachrichten an den FPolicy-Server Gibt das Zeitintervall in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Bei denen 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 ist `0`, Die Option ist deaktiviert und Keep-Alive-Nachrichten werden nicht an die FPolicy-Server gesendet. Die Standardeinstellung lautet `120s`.	`-keep-alive-interval-integer`[H m m m V natürlich]
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`. Die Standardeinstellung lautet `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 Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Anschließend wird während der erneuten Verbindungsversuche eine neue Sitzungs-ID an den FPolicy-Server gesendet. Wenn die Verbindung zwischen dem Speicher-Controller und dem FPolicy-Server beendet wird und eine erneute Verbindung innerhalb des hergestellt wird `-session-timeout` Intervall wird die alte Session-ID an den FPolicy Server gesendet, damit es Antworten für alte Benachrichtigungen senden kann. Der Standardwert ist 10 Sekunden.	`-session-timeout` [`integer`H][`integer`M][`integer`S]

Weitere Informationen zum Konfigurieren von FPolicy-externen 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. Sie dürfen dieses Zertifikat nicht löschen, während alle 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, das zum Signieren des FPolicy-Server-Zertifikats verwendet wird, wird mithilfe der installiert `security certificate install` Befehl mit dem `-type` Parameter auf gesetzt `client-ca`. Der für die Authentifizierung der SVM erforderliche private Schlüssel und das öffentliche Zertifikat werden mithilfe des installiert `security certificate install` Befehl mit dem `-type` Parameter auf gesetzt `server`.

Zertifikate replizieren sich in SVM Disaster-Recovery-Beziehungen nicht mit einer Konfiguration, die keine IDs enthält

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 eine SVM Disaster-Recovery-Beziehung einrichten, wählen Sie den Wert für `-identity -preserve` Option des `snapmirror create` Der Befehl bestimmt die Konfigurationsdetails, die in der Ziel-SVM repliziert werden.

Wenn Sie die einstellen `-identity-preserve` Option auf `true` (ID-Preserve) werden alle FPolicy Konfigurationsdetails repliziert, einschließlich der Informationen zum Sicherheitszertifikat. Sie müssen die Sicherheitszertifikate nur auf dem Ziel installieren, wenn Sie die Option auf festlegen `false` (Nicht-ID-Preserve).

Einschränkungen für externe Cluster-Scoped FPolicy 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.

Füllen Sie das Konfigurationsarbeitsblatt für die externe FPolicy Engine aus

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

Planen Sie die FPolicy Event-Konfiguration im Überblick

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 ab ONTAP 9.15.1 SMB, NFSv3, NFSv4 und 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 Parametern (`-protocol`, `-file-operations`, `-filters`). Die folgenden Kombinationen gelten für die drei Parameter:
>
> - Sie können den angeben `-protocol` Und `-file-operations` Parameter.
> - 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` Bis `z` • `A` Bis `Z` • `0` Bis `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`, Dann müssen Sie einen gültigen Wert im angeben `-file-operations` Parameter. 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 von allen Client-Anforderungen mithilfe des in angegebenen Protokolls `-protocol` Parameter. 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 Dateischließvorgänge • `create` Für Dateiererstellungsprozesse • `create-dir` Erstellen von Verzeichnisvorgängen • `delete` Für Dateilösch-Vorgänge • `delete_dir` Für Vorgänge zum Löschen von Verzeichnissen • `getattr` Für get-Attributvorgänge • `link` Für Verbindungsvorgänge • `lookup` Für Suchvorgänge • `open` Für Dateiöffnungsprozesse • `read` Für Dateilesevorgänge • `write` Für Dateischreibvorgänge • `rename` Für Dateiumbenennung • `rename_dir` Für Verzeichnisumbenennung • `setattr` Für Set-Attributvorgänge • `symlink` Für symbolische Link-Vorgänge Wenn Sie angeben `-file-operations`, Dann müssen Sie ein gültiges Protokoll im angeben `-protocol` Parameter.	`-file-operations file_operations,...`

Filter Gibt die Liste der Filter für einen bestimmten Dateivorgang für das angegebene Protokoll an. Die Werte in `-filters` Mit dem Parameter werden Client-Anforderungen gefiltert. Die Liste kann eine oder mehrere der folgenden Elemente enthalten: Wenn Sie den angeben `-filters` Parameter, dann müssen Sie auch gültige Werte für das angeben `-file -operations` Und `-protocol` Parameter. • `monitor-ads` Option zum Filtern der Clientanforderung nach alternativen Datenströmen. • `close-with-modification` Option zum Filtern der Clientanfrage nach Abschluss mit Änderung. • `close-without-modification` Option zum Filtern der Clientanfrage nach Abschluss ohne Änderung. • `first-read` Option zum Filtern der Client-Anforderung nach dem ersten Lesen. • `first-write` Option zum Filtern der Client-Anforderung nach dem ersten Schreibvorgang. • `offline-bit` Option zum Filtern der Client-Anforderung nach Offline-Bit-Set. 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 „Open with delete Intent“. 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 die `FILE_DELETE_ON_CLOSE` Flag ist angegeben. • `open-with-write-intent` Option zum Filtern der Client-Anforderung 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 Schreiben mit Größenänderung. • `setattr-with-owner-change` Option zum Filtern der Client-setattr-Anforderungen zum Ändern des Inhabers 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. Die Standardeinstellung lautet `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 Verzeichnisvorgängen.

Unterstützte Dateioperationen und Filterkombinationen, die FPolicy für SMB überwachen kann

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

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 FPolicy für NFSv3 überwachen kann

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 die 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 bei 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 FPolicy für NFSv4 überwachen kann

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

Füllen Sie das Arbeitsblatt für die FPolicy Event-Konfiguration aus

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

Planen Sie die FPolicy-Konfiguration im Überblick

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

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

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

Sie können auch mehrere optionale Richtlinieneinstellungen konfigurieren.

Was die FPolicy-Konfiguration enthält

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

Informationstyp	Option	Erforderlich	Standard
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` Bis `z` • `A` Bis `Z` • `0` Bis `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 angeben `native` Als Wert. • 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 eingestellt auf `true`, Dateizugriffsereignisse werden verweigert. • Wenn eingestellt auf `false`, Dateizugriffsereignisse sind erlaubt.	`-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 Daten-LIFs für die Verbindung mit den FPolicy Servern müssen konfiguriert werden `cifs` Als eines der zulässigen Protokolle. 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\user Name`“ verwenden. • Wenn `-allow -privileged -access` Ist auf festgelegt `no`, Jeder für diesen Parameter eingestellte Wert wird 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 FPolicy-Konfigurationen, wenn die FPolicy die native Engine verwendet

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

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

Wenn eine FPolicy, die die native Engine nutzt, auf einem Share oder Volume und dem aktiviert wird `-is-file-extension-check-on-directories-enabled` Parameter ist auf festgelegt `false` Für den Umfang der Richtlinie 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 erfolgreich ist, wenn Sie die native Engine verwenden, müssen Sie den festlegen `-is-file-extension-check-on-directories-enabled` Parameter Bis `true` Beim Erstellen des Anwendungsbereichs.

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

- Wenn diese Option aktiviert ist, stellen die FPolicy-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.

Füllen Sie das FPolicy-Arbeitsblatt aus

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

Informationstyp	Einschließlich	Ihre Werte
Name der Storage Virtual Machine (SVM	Ja.	
Name der Richtlinie	Ja.	
Ereignisnamen	Ja.	
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

Planen Sie die FPolicy Scope-Konfiguration im Überblick

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 ein Share in das enthalten ist `-shares-to-include` Parameter und das übergeordnete Volumen des Share sind in enthalten `-volumes-to-exclude` Parameter, `-volumes-to-exclude` Hat Vorrang vor `-shares-to-include`.
- Wenn eine Exportrichtlinie in enthalten ist `-export-policies-to-include` Parameter und das übergeordnete Volume der Exportrichtlinie sind in enthalten `-volumes-to-exclude` Parameter, `-volumes-to-exclude` Hat Vorrang vor `-export-policies-to-include`.
- Ein Administrator kann beides angeben `-file-extensions-to-include` Und `-file-extensions -to-exclude` Listen.

  Der `-file-extensions-to-exclude` Der Parameter wird vor dem geprüft `-file-extensions-to -include` Parameter ist aktiviert.

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 „` enthalten?`" and "*`“. 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 festgelegt ist `true`, Die Verzeichnisobjekte werden den gleichen Erweiterungsprüfungen unterzogen wie normale Dateien. Wenn dieser Parameter auf festgelegt ist `false`, Die Verzeichnisnamen sind nicht für Erweiterungen abgestimmt und Benachrichtigungen werden für Verzeichnisse gesendet, auch wenn ihre Namenserweiterungen nicht übereinstimmen. Wenn die FPolicy, der der Bereich zugewiesen ist, für die Verwendung der nativen Engine konfiguriert ist, muss dieser Parameter auf festgelegt werden `true`.	`-is-file-extension -check-on-directories -enabled` {`true`. `false`}

Füllen Sie das FPolicy Scope-Arbeitsblatt aus

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		

Erstellen Sie die FPolicy-Konfiguration

Erstellen Sie die externe FPolicy Engine

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 macht und managt. Wenn Ihre Konfiguration die interne ONTAP Engine (die native externe Engine) für einfaches Blockieren von Dateien verwendet, müssen Sie keine separate FPolicy externe Engine konfigurieren und müssen diesen Schritt nicht ausführen.

Was Sie benötigen

Der "Externer Motor" Arbeitsblatt sollte ausgefüllt werden.

Über diese Aufgabe

Wenn die externe Engine in einer MetroCluster-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.

Schritte

1. Erstellen Sie die FPolicy-externe Engine mit dem `vserver fpolicy policy external-engine create` Befehl.

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

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

2. Überprüfen Sie die Konfiguration der externen FPolicy-Engine mit dem `vserver fpolicy policy external-engine show` Befehl.

   Mit dem folgenden Befehl werden Informationen zu allen auf SVM vs1.example.com konfigurierten externen Engines angezeigt:

   ```
   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
```

Mit dem folgenden Befehl werden ausführliche Informationen zur externen Engine mit dem Namen „`Engine1`“ auf SVM vs1.example.com angezeigt:

```
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: -
```

Erstellen Sie das FPolicy-Ereignis

Wenn Sie eine FPolicy-Konfiguration erstellen, müssen Sie ein FPolicy-Ereignis erstellen. Sie verknüpfen das Ereignis mit der FPolicy, wenn es erstellt wird. Ein Ereignis definiert, welches Protokoll überwacht werden soll und welche Dateizugriffsereignisse überwacht und gefiltert werden müssen.

Bevor Sie beginnen

Sie sollten das FPolicy Event absolvieren"Arbeitsblatt".

Erstellen Sie das FPolicy-Ereignis

1. Erstellen Sie das FPolicy-Ereignis mit `vserver fpolicy policy event create` Befehl.

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

2. Überprüfen Sie die FPolicy-Event-Konfiguration mit `vserver fpolicy policy event show` Befehl.

```
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
```

Erstellen Sie die Ereignisse, bei denen der FPolicy Zugriff verweigert wird

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.

1. Erstellen Sie das FPolicy-Ereignis mit `vserver fpolicy policy event create` Befehl.

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

Erstellung von persistenten FPolicy-Speichern

Persistente Speicher können die Client-I/O-Verarbeitung von der FPolicy-Benachrichtigungsverarbeitung entkoppeln, um die Client-Latenz zu verringern. Ab ONTAP 9.14.1 ist die Einrichtung mit FPolicy möglich "Persistente Speicher" So erfassen Sie Dateizugriffsereignisse für asynchrone, nicht obligatorische Richtlinien in der SVM: Synchrone (obligatorische oder nicht obligatorische) und asynchrone obligatorische Konfigurationen werden nicht unterstützt.

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

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

- ONTAP 9.15.1 oder höher: Wenn Sie den persistenten Speicher erstellen, erstellt und konfiguriert ONTAP automatisch sein Volume gleichzeitig. Dies vereinfacht die Konfiguration des persistenten FPolicy Speichers und implementiert alle Best Practices.
- ONTAP 9.14.1: Manuelles Erstellen und Konfigurieren eines Volumes und anschließende Erstellung 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 verwenden Sie die `fpolicy persistent-store create` Befehl zum Erstellen des

persistenten FPolicy-Speichers bei Inline-Volume-Erstellung und -Konfiguration. ONTAP blockiert das Volume automatisch vom externen Benutzerprotokollzugriff (CIFS/NFS).

Bevor Sie beginnen

- Die SVM, auf der Sie den persistenten Speicher erstellen möchten, muss über mindestens ein Aggregat verfügen.
- Sie sollten Zugriff auf die für die SVM verfügbaren Aggregate und ausreichende Berechtigungen zum Erstellen von Volumes haben.

Schritte

1. Erstellen des persistenten Speichers, 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 Speicher-Volume.

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

   - Der `size` Der Parameter basiert auf der Dauer, für die die Ereignisse, die nicht an den externen Server (Partneranwendung) geliefert werden, fortgeführt werden sollen.

     Wenn Sie beispielsweise möchten, dass in einem Cluster 30 Minuten Ereignisse mit einer Kapazität von 30.000 Benachrichtigungen pro Sekunde erhalten bleiben:

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

     Um die ungefähre Benachrichtigungsrate zu ermitteln, können Sie sich entweder mit Ihrer FPolicy Partnerapplikation in Verbindung setzen oder den FPolicy-Zähler verwenden `requests_dispatched_rate`.

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

   - Der `autosize-mode` Der Parameter gibt den Autosize-Modus für das Volume an. Folgende Modi werden unterstützt:
     - Aus - das Volumen vergrößert oder verkleinert sich nicht als Antwort auf die Menge des belegten Speicherplatzes.
     - Vergrößern - das Volumen wächst automatisch, wenn der verwendete Platz im Volumen über der Wachstumsschwelle liegt.
     - Grow_Shrink - das Volumen vergrößert oder verkleinert sich als Antwort auf die Menge des genutzten Speicherplatzes.
2. Erstellen Sie die FPolicy-Richtlinie, und fügen Sie dieser Richtlinie den Namen des persistenten Speichers

hinzu. Weitere Informationen finden Sie unter "Erstellen Sie die FPolicy".

Persistenten Speicher erstellen (ONTAP 9.14.1)

Sie können ein Volume erstellen und anschließend einen persistenten Speicher zur Verwendung dieses Volumes erstellen. Anschließend können Sie das neu erstellte Volume vom externen Benutzerprotokollzugriff (CIFS/NFS) sperren.

Schritte

1. Erstellen Sie ein leeres Volume auf der SVM, 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 (mit dem cli-Befehl des Volumes oder der REST-API) der gewünschten Größe erstellt und den Namen dieses Volumes als bereitstellt `-volume` Erstellen Sie im persistenten Speicher einen CLI-Befehl oder eine REST-API.

   - Der `vserver` Parameter ist der Name der SVM.
   - Der `volume` Parameter ist der Name des persistenten Speicher-Volume.
   - Der `state` Der Parameter sollte auf „Online“ gesetzt werden, damit das Volume zur Verwendung verfügbar ist.
   - Der `policy` Der Parameter wird auf die FPolicy-Service-Richtlinie festgelegt, sofern bereits ein Parameter konfiguriert ist. Wenn nicht, können Sie den verwenden `volume modify` Befehl später, um die Richtlinie hinzuzufügen.
   - Der `unix-permissions` Parameter ist optional.
   - Der `size` Der Parameter basiert auf der Dauer, für die die Ereignisse, die nicht an den externen Server (Partneranwendung) geliefert werden, fortgeführt werden sollen.

     Wenn Sie beispielsweise möchten, dass in einem Cluster 30 Minuten Ereignisse mit einer Kapazität von 30.000 Benachrichtigungen pro Sekunde erhalten bleiben:

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

   Um die ungefähre Benachrichtigungsrate zu ermitteln, können Sie sich entweder mit Ihrer FPolicy Partnerapplikation in Verbindung setzen oder den FPolicy-Zähler verwenden `requests_dispatched_rate`.

   - Der Parameter Aggregate ist für FlexVol Volumes erforderlich, andernfalls ist er nicht erforderlich.
   - Der `snapshot-policy` Der Parameter muss auf „Keine“ gesetzt werden. Dadurch wird sichergestellt, dass keine versehentliche Wiederherstellung des Snapshots zum Verlust aktueller Ereignisse führt und eine mögliche doppelte Ereignisverarbeitung verhindert wird.

     Wenn Sie ein vorhandenes, leeres Volume verwenden möchten, verwenden Sie die `volume show` Befehl, um es und die zu finden `volume modify` Befehl, um alle erforderlichen Änderungen vorzunehmen. Stellen Sie die Richtlinie, die Größe und sicher `snapshot-policy` Die Parameter werden für den persistenten Speicher korrekt eingestellt.

2. 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 Speicher-Volume.
3. Erstellen Sie die FPolicy-Richtlinie, und fügen Sie dieser Richtlinie den Namen des persistenten Speichers hinzu. Weitere Informationen finden Sie unter "Erstellen Sie die FPolicy".

Erstellen Sie die FPolicy

Wenn Sie die FPolicy erstellen, verknüpfen Sie eine externe Engine und ein oder mehrere Ereignisse mit der Richtlinie. Die Richtlinie legt außerdem fest, ob ein obligatorisches Screening 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.

Was Sie benötigen

- Das Arbeitsblatt für die FPolicy sollte ausgefüllt werden.
- Wenn Sie planen, die Richtlinie für FPolicy-Server zu konfigurieren, muss die externe Engine vorhanden sein.
- Mindestens ein FPolicy-Ereignis, das Sie auf eine Verknüpfung mit der FPolicy planen, muss existieren.
- Wenn Sie einen privilegierten Datenzugriff konfigurieren möchten, muss auf der SVM ein SMB-Server vorhanden sein.
- Um einen persistenten Speicher für eine Policy zu konfigurieren, muss der Engine-Typ **async** sein und die Policy muss **non-obligatorische** sein.

  Weitere Informationen finden Sie unter "Erstellen persistenter Speicher".

Schritte

1. Erstellen der FPolicy:

   ```
   vserver fpolicy policy create -vserver-name vserver_name -policy-name
   policy_name -engine engine_name -events event_name, [-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 ein oder mehrere Events zur FPolicy hinzufügen.
   - Standardmäßig ist das obligatorische Screening aktiviert.
   - Wenn Sie privilegierten Zugriff zulassen möchten, setzen Sie die ein `-allow-privileged-access` Parameter an `yes`, Sie müssen auch einen privilegierten Benutzernamen für privilegierten Zugriff konfigurieren.
   - Wenn Sie Passthrough-read konfigurieren möchten, indem Sie die einstellen `-is-passthrough -read-enabled` Parameter an `true`, Sie müssen auch privilegierten Datenzugriff konfigurieren.

Mit dem folgenden Befehl wird eine Richtlinie mit dem Namen „`policy1`“ erstellt, in der das Ereignis „`event1`“ und die externe Engine „`Engine1`“ mit ihr verknüpft sind. Diese Richtlinie verwendet Standardwerte in der Richtlinienkonfiguration: `vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

Mit dem folgenden Befehl wird eine Richtlinie mit dem Namen „`policy2`“ erstellt, in der das Ereignis „`event2`“ und die externe Engine „`Engine2`“ mit ihr verknüpft sind. Diese Richtlinie wurde für die Verwendung von privilegiertem Zugriff unter Verwendung des angegebenen Benutzernamens konfiguriert. 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
```

Mit dem folgenden Befehl wird eine Richtlinie mit dem Namen „`nativ1`“ erstellt, die das Ereignis „`event3`“ mit ihr verknüpft hat. 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. Überprüfen Sie die FPolicy-Konfiguration mit `vserver fpolicy policy show` Befehl.

   Mit dem folgenden Befehl werden Informationen zu den drei konfigurierten FPolicy-Richtlinien angezeigt, einschließlich der folgenden Informationen:

   - Der Richtlinie zugeordnete SVM
   - Die externe Engine, die der Richtlinie zugeordnet ist
   - Die mit der Richtlinie verbundenen Ereignisse
   - Gibt an, ob eine obligatorische Überprüfung erforderlich ist
   - Gibt an, 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
```

Erstellen Sie den FPolicy-Bereich

Nachdem Sie die FPolicy erstellt haben, müssen Sie einen FPolicy-Bereich erstellen. Bei der Erstellung des Anwendungsbereichs verknüpfen Sie den Geltungsbereich mit einer FPolicy. Ein Geltungsbereich definiert die Grenzen, für die die FPolicy gilt. Scopes können Dateien einschließen oder ausschließen, die auf Freigaben, Exportrichtlinien, Volumes und Dateierweiterungen basieren.

Was Sie benötigen

Das FPolicy Scope-Arbeitsblatt muss ausgefüllt werden. Die FPolicy muss mit einer zugeordneten externen Engine existieren (wenn die Richtlinie zur Verwendung externer FPolicy-Server konfiguriert ist) und über mindestens ein damit verbundener FPolicy-Ereignis verfügen.

Schritte

1. Erstellen Sie den FPolicy-Bereich mit `vserver fpolicy policy scope create` Befehl.

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

2. Überprüfen Sie die FPolicy-Scope-Konfiguration mit `vserver fpolicy policy scope show` Befehl.

   ```
   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: -
   ```

Aktivieren Sie die FPolicy

Nachdem Sie eine FPolicy-Konfiguration durchlaufen haben, aktivieren Sie die FPolicy. Durch das Aktivieren der Richtlinie wird die Priorität festgelegt und die Dateizugriffsüberwachung für die Richtlinie gestartet.

Was Sie benötigen

Die FPolicy muss mit einer zugeordneten externen Engine existieren (wenn die Richtlinie zur Verwendung externer FPolicy-Server konfiguriert ist) und über mindestens ein damit verbundener FPolicy-Ereignis verfügen. Der Richtlinienumfang von FPolicy muss vorhanden sein und der FPolicy 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 Ereignis für den Dateizugriff abonniert hat. Richtlinien, die die native Engine-Konfiguration verwenden, haben für jede andere Engine eine höhere Priorität als Richtlinien, unabhängig von der ihnen bei der Aktivierung der Richtlinie zugewiesenen Sequenznummer.

> Eine Richtlinie kann auf der Admin-SVM nicht aktiviert werden.

Schritte

1. Aktivieren Sie die FPolicy mithilfe von `vserver fpolicy enable` Befehl.

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

2. Überprüfen Sie, ob die FPolicy mit aktiviert wird `vserver fpolicy show` Befehl.

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

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

Managen von FPolicy-Konfigurationen

Ändern Sie FPolicy-Konfigurationen

Befehle zum Ändern von FPolicy-Konfigurationen

Sie können FPolicy-Konfigurationen ändern, indem Sie die Elemente ändern, aus denen die Konfiguration besteht. Sie können externe Engines, FPolicy-Ereignisse, FPolicy Scopes, persistente FPolicy-Speicher und FPolicy-Richtlinien ändern. Sie können FPolicy auch aktivieren oder deaktivieren. Wenn Sie die FPolicy deaktivieren, wird die Dateiüberwachung für diese Richtlinie eingestellt.

Sie sollten eine FPolicy-Richtlinie deaktivieren, bevor Sie die Konfiguration ändern.

Sie möchten Folgendes ändern:	Befehl
Externe Motoren	`vserver fpolicy policy external-engine modify`
Veranstaltungen	`vserver fpolicy policy event modify`
Bereich	`vserver fpolicy policy scope modify`
Persistenter Speicher	`vserver fpolicy persistent-store modify`
Richtlinien	`vserver fpolicy policy modify`

Weitere Informationen zu den Befehlen finden Sie auf den man-Pages.

Aktivieren oder Deaktivieren von FPolicy-Richtlinien

Sie können FPolicy-Richtlinien aktivieren, nachdem die Konfiguration abgeschlossen ist. Durch das Aktivieren der Richtlinie wird die Priorität festgelegt und die Dateizugriffsüberwachung für die Richtlinie gestartet. Sie können FPolicy-Richtlinien

deaktivieren, wenn Sie die Dateizugriffsüberwachung für die Richtlinie beenden möchten.

Was Sie benötigen

Vor Aktivierung von FPolicy Richtlinien 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 Ereignis für den Dateizugriff abonniert hat.
- Richtlinien, die die native Engine-Konfiguration verwenden, haben für jede andere Engine eine höhere Priorität als Richtlinien, unabhängig von der ihnen bei der Aktivierung der Richtlinie zugewiesenen Sequenznummer.
- Wenn Sie die Priorität einer FPolicy ändern möchten, müssen Sie die Richtlinie deaktivieren und dann mithilfe der neuen Sequenznummer erneut aktivieren.

Schritt

1. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Aktivieren einer FPolicy	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`
Deaktivieren Sie eine FPolicy	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

Zeigen Sie Informationen zu FPolicy-Konfigurationen an

Funktionsweise der Befehle show

Es ist hilfreich beim Anzeigen von Informationen über die FPolicy Konfiguration, um zu verstehen, wie das `show` Befehle funktionieren.

A `show` Durch Befehl ohne zusätzliche Parameter werden Informationen in einem Übersichtsformular angezeigt. Zusätzlich alle `show` Der Befehl weist die beiden gleichen optionalen Parameter auf, die sich gegenseitig ausschließen. `-instance` Und `-fields`.

Wenn Sie das verwenden `-instance` Parameter mit A `show` Mit dem Befehl werden in der Ausgabe des Befehls detaillierte Informationen in einem Listenformat angezeigt. In einigen Fällen kann die detaillierte Ausgabe langwierig sein und mehr Informationen enthalten, als Sie benötigen. Sie können das verwenden `-fields fieldname[,fieldname…]` Parameter, um die Ausgabe so anzupassen, dass nur Informationen für die von Ihnen angegebenen Felder angezeigt werden. Sie können bestimmen, welche Felder Sie angeben können, indem Sie sie eingeben `?` Nach dem `-fields` Parameter.

> Die Ausgabe von A `show` Befehl mit dem `-fields` Der Parameter zeigt möglicherweise weitere relevante und notwendige Felder in Bezug auf die angeforderten Felder an.

Alle `show` Befehl enthält mindestens einen optionalen Parameter, der die Ausgabe filtert und Sie können den Umfang der in der Befehlsausgabe angezeigten Informationen eingrenzen. Sie können festlegen, welche optionalen Parameter für einen Befehl zur Verfügung stehen, indem Sie eingeben `?` Nach dem `show` Befehl.

Der `show` Der Befehl unterstützt UNIX-Style-Muster und Wildcards, damit Sie in Argumenten mit Befehlsparametern mehrere Werte erfüllen können. Sie können beispielsweise den Platzhalter-Operator (*), DEN OPERATOR NOT (!), DEN OPERATOR ODER (\<), den Bereichsoperator (integer…integer), den kleiner-als-Operator (<), den größer-als-Operator (>), den Operator kleiner oder gleich (=) und den Operator größer oder gleich (>=) verwenden, wenn Sie Werte angeben.

Weitere Informationen zur Verwendung von UNIX-Stilmustern und Wildcards finden Sie im Über die ONTAP Befehlszeilenschnittstelle.

Befehle zum Anzeigen von Informationen zu FPolicy-Konfigurationen

Sie verwenden das `fpolicy show` Befehle zum Anzeigen von Informationen zur FPolicy Konfiguration, einschließlich Informationen zu externen FPolicy Engines, Ereignissen, Scopes und Richtlinien.

Wenn Sie Informationen über FPolicy anzeigen möchten…	Befehl
Externe Motoren	`vserver fpolicy policy external-engine show`
Veranstaltungen	`vserver fpolicy policy event show`
Bereich	`vserver fpolicy policy scope show`
Richtlinien	`vserver fpolicy policy show`

Weitere Informationen zu den Befehlen finden Sie auf den man-Pages.

Zeigt Informationen zum FPolicy-Status an

Sie können Informationen zum Status von FPolicy anzeigen, um zu bestimmen, ob eine Richtlinie aktiviert ist, welche externe Engine sie konfiguriert hat, welche Sequenznummer sie für die Richtlinie ist und welcher Storage Virtual Machine (SVM) die FPolicy zugeordnet ist.

Über diese Aufgabe

Wenn Sie keine Parameter angeben, werden mit dem Befehl die folgenden Informationen angezeigt:

- SVM-Name
- Name der Richtlinie
- Police-Sequenznummer
- Der Richtlinienstatus

Zusätzlich zum Anzeigen von Informationen zum Richtlinienstatus für auf dem Cluster oder einer bestimmten SVM konfigurierte Richtlinien können Sie mit Befehlsparametern die Ausgabe des Befehls anhand anderer Kriterien filtern.

Sie können den angeben `-instance` Parameter zum Anzeigen detaillierter Informationen zu aufgeführten

Richtlinien Alternativ können Sie den verwenden `-fields` Parameter, mit dem nur die angegebenen Felder in der Befehlsausgabe oder angezeigt werden sollen `-fields ?` Um zu bestimmen, welche Felder Sie verwenden können.

Schritt

1. Zeigt gefilterte Informationen zum Richtlinienstatus mithilfe des entsprechenden Befehls an:

Wenn Sie Statusinformationen zu Richtlinien anzeigen möchten…	Geben Sie den Befehl ein…
Auf dem Cluster	`vserver fpolicy show`
Die den angegebenen Status aufweisen	`vserver fpolicy show -status {on
off}`	Auf einer angegebenen 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

Im folgenden Beispiel werden die Informationen über FPolicy-Richtlinien auf dem Cluster angezeigt:

```
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
```

Zeigen Sie Informationen zu aktivierten FPolicy-Richtlinien an

Sie können Informationen über aktivierte FPolicy Richtlinien anzeigen, um zu bestimmen, welche FPolicy externe Engine sie zu verwenden konfiguriert ist, welche Priorität für die Richtlinie hat und zu welcher Storage Virtual Machine (SVM) die FPolicy zugeordnet ist.

Über diese Aufgabe

Wenn Sie keine Parameter angeben, werden mit dem Befehl die folgenden Informationen angezeigt:

- SVM-Name
- Name der Richtlinie
- Richtlinienpriorität

Sie können mit den Befehlsparametern die Ausgabe des Befehls nach bestimmten Kriterien filtern.

Schritt

1. Informationen über aktivierte FPolicy-Richtlinien werden mit dem entsprechenden Befehl angezeigt:

Wenn Informationen über aktivierte Richtlinien angezeigt werden sollen…	Geben Sie den Befehl ein…
Auf dem Cluster	`vserver fpolicy show-enabled`
Auf einer angegebenen 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

Im folgenden Beispiel werden die Informationen über aktivierte FPolicy-Richtlinien auf dem Cluster angezeigt:

```
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
```

Verwalten von FPolicy-Serververbindungen

Verbindung zu externen FPolicy-Servern herstellen

Um die Dateiverarbeitung zu aktivieren, müssen Sie möglicherweise manuell eine Verbindung zu einem externen FPolicy-Server herstellen, wenn die Verbindung zuvor beendet wurde. Eine Verbindung wird beendet, nachdem das Server-Timeout erreicht wurde oder aufgrund eines Fehlers. Alternativ kann der Administrator eine Verbindung manuell beenden.

Über diese Aufgabe

Wenn ein schwerwiegender Fehler auftritt, kann die Verbindung zum FPolicy-Server beendet werden. Nachdem Sie das Problem behoben haben, das den schwerwiegenden Fehler verursacht hat, müssen Sie eine manuelle Verbindung zum FPolicy-Server herstellen.

Schritte

1. Stellen Sie eine Verbindung mit dem externen FPolicy-Server her `vserver fpolicy engine-connect` Befehl.

   Weitere Informationen zum Befehl finden Sie in den man-Pages.

2. Überprüfen Sie, ob der externe FPolicy-Server mit dem verbunden ist `vserver fpolicy show-engine` Befehl.

   Weitere Informationen zum Befehl finden Sie in den man-Pages.

Verbindung zu externen FPolicy-Servern trennen

Möglicherweise müssen Sie die Verbindung zu einem externen FPolicy Server manuell trennen. Dies kann wünschenswert sein, wenn der FPolicy Server Probleme mit der Bearbeitung von Benachrichtigungsanfragen hat oder wenn Sie Wartungsarbeiten auf dem FPolicy-Server durchführen müssen.

Schritte

1. Trennen Sie die Verbindung mit dem vom externen FPolicy-Server `vserver fpolicy engine-disconnect` Befehl.

   Weitere Informationen zum Befehl finden Sie in den man-Pages.

2. Überprüfen Sie, ob der externe FPolicy-Server mit dem getrennt wird `vserver fpolicy show-engine` Befehl.

   Weitere Informationen zum Befehl finden Sie in den man-Pages.

Zeigen Sie Informationen über Verbindungen zu externen FPolicy-Servern an

Sie können Statusinformationen über Verbindungen zu externen FPolicy Servern (FPolicy-Servern) für das Cluster oder für eine angegebene Storage Virtual Machine (SVM) anzeigen. Diese Informationen können Ihnen dabei helfen, festzustellen, welche FPolicy Server verbunden sind.

Über diese Aufgabe

Wenn Sie keine Parameter angeben, werden mit dem Befehl die folgenden Informationen angezeigt:

- SVM-Name
- Node-Name
- FPolicy-Name
- FPolicy-Server-IP-Adresse
- FPolicy-Serverstatus

- FPolicy-Servertyp

Zusätzlich zum Anzeigen von Informationen über FPolicy-Verbindungen auf dem Cluster oder einer bestimmten SVM können Sie mit Befehlsparametern die Ausgabe des Befehls um andere Kriterien filtern.

Sie können den angeben `-instance` Parameter zum Anzeigen detaillierter Informationen zu aufgeführten Richtlinien Alternativ können Sie den verwenden `-fields` Parameter, um nur die angegebenen Felder in der Befehlsausgabe anzuzeigen. Sie können eingeben `?` Nach dem `-fields` Parameter, um herauszufinden, welche Felder Sie verwenden können.

Schritt

1. Zeigen Sie gefilterte Informationen zum Verbindungsstatus zwischen dem Knoten und dem FPolicy-Server mithilfe des entsprechenden Befehls an:

Wenn Sie Verbindungsinformationen über FPolicy-Server anzeigen möchten…	Eingeben…
Die Sie angeben	`vserver fpolicy show-engine -server IP_address`
Für eine angegebene SVM	`vserver fpolicy show-engine -vserver vserver_name`
Die mit einer angegebenen Richtlinie verbunden sind	`vserver fpolicy show-engine -policy-name policy_name`
Mit dem von Ihnen angegebenen Serverstatus	`vserver fpolicy show-engine -server-status status` Für den Serverstatus kann einer der folgenden Werte angezeigt werden: • `connected` • `disconnected` • `connecting` • `disconnecting`
Mit dem angegebenen Typ	`vserver fpolicy show-engine -server-type type` Der FPolicy-Server-Typ kann einer der folgenden sein: • `primary` • `secondary`

Die Verbindung wurde mit dem angegebenen Grund getrennt	`vserver fpolicy show-engine -disconnect-reason text` Die Verbindung kann aus mehreren Gründen erfolgen. Die folgenden Gründe sind häufig für die Verbindung: • `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 zu externen Engine-Verbindungen mit FPolicy-Servern auf SVM vs1.example.com an:

```
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
```

In diesem Beispiel werden nur Informationen zu verbundenen FPolicy-Servern angezeigt:

```
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
```

Zeigen Sie Informationen zum Verbindungsstatus der FPolicy-Durchleseverbindung an

Sie können Informationen über den FPolicy Passthrough-Read-Verbindungsstatus zu externen FPolicy Servern (FPolicy-Server) für das Cluster oder für eine angegebene

Storage Virtual Machine (SVM) anzeigen. Diese Informationen können Ihnen dabei helfen zu bestimmen, welche FPolicy-Server über Pass-Read-Datenverbindungen verfügen und für welche FPolicy-Server die Passthrough-Read-Verbindung getrennt haben.

Über diese Aufgabe

Wenn Sie keinen Parameter angeben, werden mit dem Befehl die folgenden Informationen angezeigt:

- SVM-Name
- FPolicy-Name
- Node-Name
- FPolicy-Server-IP-Adresse
- FPolicy-Verbindungsstatus beim Passthrough-Lesen

Zusätzlich zum Anzeigen von Informationen über FPolicy-Verbindungen auf dem Cluster oder einer bestimmten SVM können Sie mit Befehlsparametern die Ausgabe des Befehls um andere Kriterien filtern.

Sie können den angeben `-instance` Parameter zum Anzeigen detaillierter Informationen zu aufgeführten Richtlinien Alternativ können Sie den verwenden `-fields` Parameter, um nur die angegebenen Felder in der Befehlsausgabe anzuzeigen. Sie können eingeben `?` Nach dem `-fields` Parameter, um herauszufinden, welche Felder Sie verwenden können.

Schritt

1. Zeigen Sie gefilterte Informationen zum Verbindungsstatus zwischen dem Knoten und dem FPolicy-Server mithilfe des entsprechenden Befehls an:

Wenn Sie Informationen zum Verbindungsstatus anzeigen möchten über…	Geben Sie den Befehl ein…
FPolicy-Verbindungsstatus für Passthrough-Lesevorgang für das Cluster	`vserver fpolicy show-passthrough-read-connection`
FPolicy-Verbindungsstatus für Passthrough-Leseverbindungen für eine angegebene SVM	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`
FPolicy-Verbindungsstatus für eine bestimmte Richtlinie zum Passthrough-Lesen	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
Detaillierter Verbindungsstatus von FPolicy über Durchleseverbindungen für eine bestimmte Richtlinie	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`

FPolicy Passthrough-read Verbindungsstatus für den von Ihnen angegebenen Status	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status` Für den Serverstatus kann einer der folgenden Werte angezeigt werden: • `connected` • `disconnected`

Beispiel

Mit dem folgenden Befehl werden Informationen zu Passthrough-Read-Verbindungen von allen FPolicy-Servern im Cluster angezeigt:

```
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
```

Mit dem folgenden Befehl werden ausführliche Informationen zu PassThrough-Read-Verbindungen von FPolicy-Servern angezeigt, 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
```