



FPolicy verstehen

ONTAP 9

NetApp
May 09, 2024

Inhalt

- FPolicy verstehen 1
 - Was die beiden Teile der FPolicy Lösung sind 1
 - Was sind synchrone und asynchrone Benachrichtigungen 1
 - FPolicy persistente Speicher 2
 - FPolicy-Konfigurationstypen 3
 - Rollen, die Cluster-Komponenten bei FPolicy Implementierung spielen 5
 - Wie FPolicy mit externen FPolicy-Servern funktioniert 5
 - Was ist der Kommunikationsprozess zwischen Knoten und externem FPolicy-Server 7
 - So funktionieren FPolicy Services über SVM-Namespaces hinweg 9
 - FPolicy Passthrough-Read verbessert die Benutzerfreundlichkeit für hierarchisches Storage-
Management 9

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

Dateizugriffseignisse 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

Ab ONTAP 9.14.1 können Sie mit FPolicy einen persistenten Speicher einrichten, um Dateizugriffseignisse 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.

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.

Best Practices in sich vereint

Cluster-Administratoren müssen ein Volume für den persistenten Speicher jeder SVM konfigurieren, für die FPolicy aktiviert ist. Bei der Konfiguration erfasst ein persistenter Speicher alle übereinstimmenden FPolicy-

Ereignisse, die weiter in der FPolicy-Pipeline verarbeitet und an den externen Server gesendet werden.

Der persistente Speicher bleibt so, wie er zu dem Zeitpunkt war, zu dem das letzte Ereignis empfangen wurde, wenn ein unerwarteter Neustart erfolgt ist, oder FPolicy wird deaktiviert und erneut aktiviert. Nach einer Übernahme werden neue Ereignisse vom Partner-Node gespeichert und 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 in derselben SVM von einem Node zu einem anderen verschoben wird, werden die noch zu verarbeitenden Benachrichtigungen auch in den neuen Node verschoben. Sie müssen den erneut ausführen `fpolicy persistent-store create` Befehl auf einem der Knoten nach dem Verschieben des Volumes, um sicherzustellen, dass die ausstehende Benachrichtigung an den externen Server gesendet wird.

Das persistente Speicher-Volume wird auf SVM-Basis eingerichtet. Sie müssen für jede FPolicy aktivierte SVM ein persistentes Speicher-Volume erstellen.

Erstellen Sie das persistente Speicher-Volume auf dem Node mit LIFs, die davon ausgehen, dass der maximale Datenverkehr durch FPolicy überwacht wird.

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.

Der Name des persistenten Speichervolumes und der zum Zeitpunkt der Volume-Erstellung angegebene Verbindungspfad müssen übereinstimmen.

Lassen Sie die Snapshot-Richtlinie auf festlegen `none` Für dieses 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.

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. Um dies zu erreichen, heben Sie nach Aktivierung von FPolicy die Bereitstellung des Volumes in ONTAP auf, um den Verbindungspfad zu entfernen. Dies macht ihn für den Benutzerprotokollzugriff unzugänglich.

Weitere Informationen 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 Dateieinstellungen.

Hinweis: Nicht ablehnte Dateieinstellungsanfragen 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 Dateierweiterung blockiert. Beispielsweise zum Blockieren von Dateien, die enthalten `mp3` Erweiterungen: Sie konfigurieren eine Richtlinie, um Benachrichtigungen für bestimmte Vorgänge mit Zielerweiterungen von `mp3` bereitzustellen. 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 Bildschirmen Dateien auf der Grundlage der Erweiterungen und nicht auf den Inhalt der Datei.
- Bei symbolischen Links verwendet das native File Blocking die Dateierweiterung der Root-Datei.

Weitere Informationen zu ["FPolicy: Native Dateisperre"](#).

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 Benachrichtungsverarbeitung 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 Sperrungen. 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.

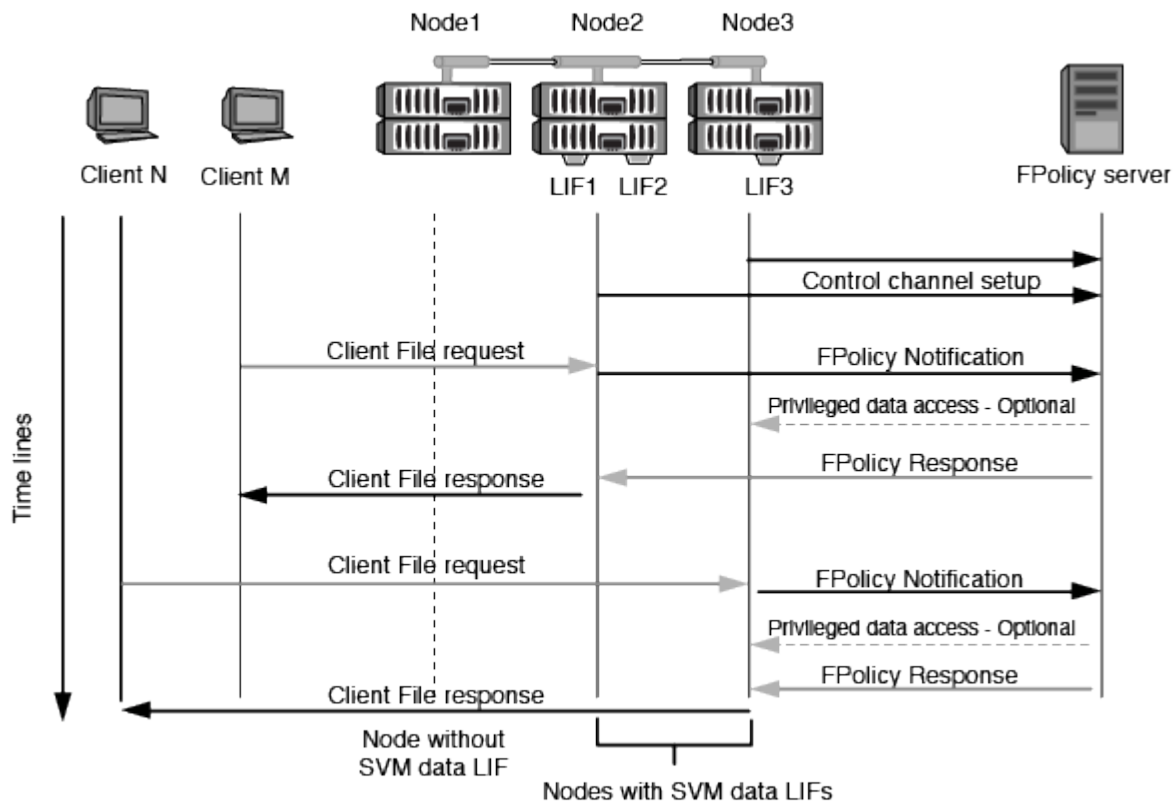
Jeder Node, der an jeder Storage Virtual Machine (SVM) teilnimmt, initiiert mithilfe von TCP/IP eine Verbindung zu einem externen FPolicy Server (FPolicy Server). Verbindungen zu den FPolicy-Servern werden mithilfe von Node-Daten-LIFs eingerichtet. Daher kann ein teilnehmender Node eine Verbindung nur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

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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