So funktioniert FPolicy

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

So funktioniert FPolicy 1
- Was die beiden Teile der FPolicy Lösung sind 1
- Was sind synchrone und asynchrone Benachrichtigungen 1
- Rollen, die Cluster-Komponenten bei FPolicy Implementierung spielen 2
- Wie FPolicy mit externen FPolicy-Servern funktioniert 3
- Was ist der Kommunikationsprozess zwischen Knoten und externem FPolicy-Server 5
- So funktionieren FPolicy Services über SVM-Namespaces hinweg 7

So funktioniert FPolicy

Was die beiden Teile der FPolicy Lösung sind

FPolicy ist ein Framework für die Dateizugriffsbenachrichtigung, mit dem Dateizugriffsereignisse auf Storage Virtual Machines (SVMs) überwacht und gemanagt werden.

Es gibt zwei Teile zu einer FPolicy Lösung. Das ONTAP FPolicy Framework managt Aktivitäten auf dem Cluster und sendet Benachrichtigungen an externe FPolicy Server. Externe FPolicy Server verarbeiten Benachrichtigungen, die von ONTAP FPolicy gesendet werden.

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.

- **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

Sie können das SDK für FPolicy verwenden, um auch andere Applikationen zu identifizieren und zu implementieren.

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

Wie FPolicy mit externen FPolicy Servern Übersicht 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

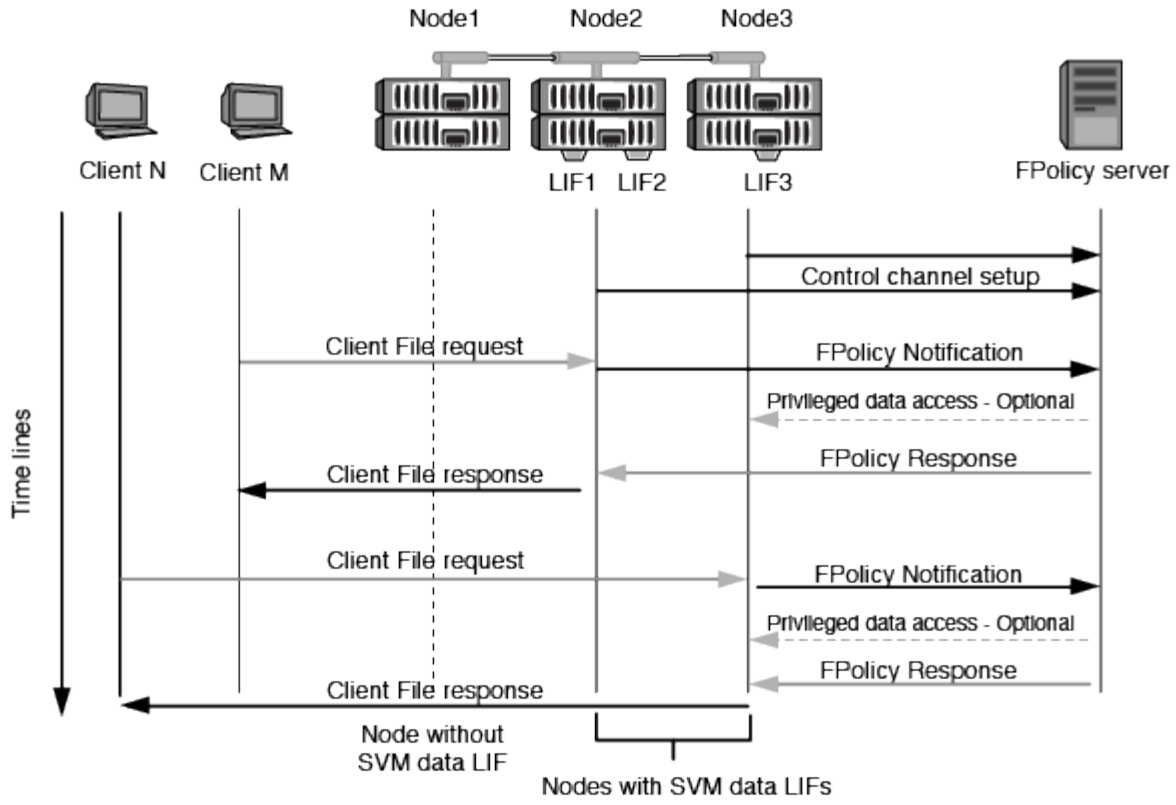
Um Ihre FPolicy-Konfiguration richtig zu planen, sollten Sie verstehen, was der Knoten-zu-externe FPolicy Server-Kommunikationsprozess ist.

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 von Cluster-Failover auf den FPolicy-Server können abgeschwächt werden, indem der LIF-Manager zur Migration des in der FPolicy Kommunikation verwendeten Daten-Ports zu einem anderen aktiven Node konfiguriert wird. Nach Abschluss der Migration wird über den neuen Daten-Port eine neue Verbindung hergestellt.

Wenn der LIF-Manager 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