Wie FPolicy mit externen FPolicy-Servern funktioniert

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

Wie FPolicy mit externen FPolicy-Servern funktioniert 1
- Wie FPolicy mit externen FPolicy Servern Übersicht funktioniert 1
- Wie Kontrollkanäle für die FPolicy Kommunikation verwendet werden 1
- Verwendung von privilegierten Datenzugriffskanälen für die synchrone Kommunikation 1
- Verwendung von FPolicy Connection Anmeldeinformationen mit privilegierten Datenzugriffskanälen 2
- Was die Gewährung von Super-User-Anmeldeinformationen für privilegierten Datenzugriff bedeutet 2
- So managt FPolicy die Richtlinienverarbeitung 2

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.