瞭解 **FPolicy**

ONTAP 9

NetApp
February 12, 2026

目錄

瞭解 FPolicy

了解ONTAP FPolicy 解決方案

FPolicy 是檔案存取通知架構、可用來透過合作夥伴解決方案監控及管理儲存虛擬機器（ SVM ）上的檔案存取事件。合作夥伴解決方案可協助您處理各種使用案例、例如資料治理與法規遵循、勒索軟體保護及資料移動性。

合作夥伴解決方案包括 NetApp 支援的第三方解決方案，以及 NetApp 產品工作負載安全性和雲端資料感測。

FPolicy解決方案有兩個部分。ONTAP FPolicy 架構可管理叢集上的活動、並傳送通知給合作夥伴應用程式（也稱為外部 FPolicy 伺服器）。外部 FPolicy 伺服器會處理 ONTAP FPolicy 傳送的通知、以履行客戶使用案例。

此解決方案可建立及維護FPolicy組態、監控檔案事件、並將通知傳送至外部FPolicy伺服器。ONTAP支援內部基礎架構、可在外部FPolicy伺服器與儲存虛擬機器（SVM）節點之間進行通訊。ONTAP

FPolicy架構會連線至外部FPolicy伺服器、並在用戶端存取導致這些事件發生時、將特定檔案系統事件的通知傳送至FPolicy伺服器。外部FPolicy伺服器會處理通知、並將回應傳回節點。通知處理的結果取決於應用程式、以及節點與外部伺服器之間的通訊是否為非同步或同步。

ONTAP FPolicy 同步與非同步通知

FPolicy會透過FPolicy介面將通知傳送至外部FPolicy伺服器。通知會以同步或非同步模式傳送。通知模式會決定ONTAP 將通知傳送至FPolicy伺服器後的功能。

- 非同步通知

  藉由非同步通知、節點不會等待FPolicy伺服器的回應、進而提升系統的整體處理量。這類通知適用於FPolicy伺服器不需要在通知評估後採取任何行動的應用程式。例如、當儲存虛擬機器（SVM）管理員想要監控和稽核檔案存取活動時、就會使用非同步通知。

  如果以非同步模式運作的FPolicy伺服器發生網路中斷、則中斷期間產生的FPolicy通知會儲存在儲存節點上。當FPolicy伺服器重新連線時、系統會警示已儲存的通知、並從儲存節點擷取通知。在停機期間可儲存通知的時間長度可設定為10分鐘。

  從 ONTAP 9.14.1 開始、 FPolicy 可讓您設定持續儲存區、以擷取 SVM 中非強制性非非同步原則的檔案存取事件。持續儲存區可協助將用戶端 I/O 處理與 FPolicy 通知處理分離、以減少用戶端延遲。不支援同步（強制或非強制）和非同步強制組態。

- 同步通知

  設定為以同步模式執行時、FPolicy伺服器必須先確認每個通知、才能繼續執行用戶端作業。此類型的通知會在根據通知評估結果需要採取行動時使用。例如、當SVM管理員想要根據外部FPolicy伺服器上指定的條件來允許或拒絕要求時、就會使用同步通知。

同步與非同步應用程式

FPolicy應用程式有許多可能的用途、包括非同步和同步。

非同步應用程式是指外部FPolicy伺服器不會改變存取儲存虛擬機器（SVM）上檔案或目錄或修改資料的方式。例如：

- 檔案存取與稽核記錄
- 儲存資源管理

同步應用程式是指資料存取遭竄改或資料遭外部FPolicy伺服器修改的應用程式。例如：

- 配額管理
- 檔案存取封鎖
- 檔案歸檔與階層式儲存管理
- 加密與解密服務
- 壓縮與解壓縮服務

ONTAP FPolicy 持久存儲

持續儲存區可協助將用戶端 I/O 處理與 FPolicy 通知處理分離、以減少用戶端延遲。從 ONTAP 9.14.1 開始、您可以設定 FPolicy 持續儲存區、以擷取 SVM 中非強制性非非同步原則的檔案存取事件。不支援同步（強制或非強制）和非同步強制組態。

此功能僅適用於 FPolicy 外部模式。您使用的合作夥伴應用程式需要支援此功能。您應與合作夥伴合作、確保支援此 FPolicy 組態。

從 ONTAP 9.15.1 開始、 FPolicy 永續性儲存區組態已簡化。。 `persistent-store create` 命令可自動建立 SVM 的 Volume 、並使用持續儲存區最佳實務做法來設定 Volume 。

如需持續儲存最佳實務做法的詳細資訊、請參閱 "設定FPolicy的需求、考量及最佳實務做法"。

如需新增持續儲存區的相關資訊、請參閱 "建立持續儲存區"。

ONTAP FPolicy 配置類型

有兩種基本的FPolicy組態類型。其中一個組態使用外部FPolicy伺服器來處理通知並根據通知採取行動。另一個組態不使用外部FPolicy伺服器、而是使用ONTAP 內部的、原生的FPolicy伺服器、根據副檔名來進行簡單的檔案封鎖。

- 外部**FPolicy**伺服器組態

  通知會傳送至FPolicy伺服器、該伺服器會篩選要求並套用規則、以判斷節點是否應允許要求的檔案操作。對於同步原則、FPolicy伺服器接著會傳送回應給節點、以允許或封鎖要求的檔案作業。

- 原生**FPolicy**伺服器組態

  通知會在內部篩選。根據在FPolicy範圍中設定的副檔名設定、允許或拒絕要求。

  附註：不記錄被拒絕的副檔名要求。

何時建立原生**FPolicy**組態

原生FPolicy組態使用ONTAP 內部的FPolicy引擎、根據檔案副檔名來監控及封鎖檔案作業。此解決方案不需要外部FPolicy伺服器（FPolicy伺服器）。當這個簡單的解決方案只是需要的時候、使用原生檔案封鎖組態是適當的做法。

原生檔案封鎖功能可讓您監控符合設定作業和篩選事件的任何檔案作業、然後拒絕存取具有特定副檔名的檔案。這是預設組態。

此組態可讓您僅根據檔案副檔名來封鎖檔案存取。例如、封鎖包含的檔案 `mp3` 副檔名時、您可以設定原則、為目標副檔名為的特定作業提供通知 `mp3`。原則設定為拒絕 `mp3` 產生通知之作業的檔案要求。

下列項目適用於原生FPolicy組態：

- FPolicy伺服器型檔案篩選所支援的相同篩選器和傳輸協定集、也支援原生檔案封鎖。
- 您可以同時設定原生檔案封鎖和FPolicy伺服器型檔案篩選應用程式。

  若要這麼做、您可以針對儲存虛擬機器（SVM）設定兩個獨立的FPolicy原則、其中一個設定為原生檔案封鎖、另一個設定為FPolicy伺服器型檔案篩選。

- 原生檔案封鎖功能只會根據副檔名而非檔案內容來篩選檔案。
- 在符號連結的情況下、原生檔案封鎖會使用根檔案的副檔名。

深入瞭解 "FPolicy：原生檔案封鎖"。

何時建立使用外部**FPolicy**伺服器的組態

使用外部FPolicy伺服器來處理及管理通知的FPolicy組態、可針對需要根據副檔名進行簡單檔案封鎖的使用案例、提供健全的解決方案。

當您想要執行監控及記錄檔案存取事件、提供配額服務、根據簡單副檔名以外的條件執行檔案封鎖、使用階層式儲存管理應用程式提供資料移轉服務等作業時、應建立使用外部FPolicy伺服器的組態、 或是提供一組精細的原則、僅監控儲存虛擬機器（SVM）中的資料子集。

ONTAP FPolicy 實作中的叢集元件角色

叢集、內含的儲存虛擬機器（SVM）和資料生命量、都在FPolicy實作中扮演著重要角色。

- 叢集

  叢集包含FPolicy管理架構、並維護及管理叢集中所有FPolicy組態的相關資訊。

- * SVM*

  FPolicy組態是在SVM層級定義。組態的範圍是SVM、它只能在SVM資源上運作。某個SVM組態無法監控及傳送針對位於另一個SVM上的資料所提出的檔案存取要求通知。

  可在管理SVM上定義FPolicy組態。在管理SVM上定義組態之後、即可在所有SVM中看到及使用這些組態。

- 資料生命量

連接至FPolicy伺服器的方式是透過屬於SVM的資料LIF與FPolicy組態。這些連線所使用的資料生命量、可能會像一般用戶端存取所使用的資料生命量一樣進行容錯移轉。

ONTAP FPolicy 如何與外部 FPolicy 伺服器搭配使用

在儲存虛擬機器（SVM）上設定並啟用FPolicy之後、FPolicy會在SVM所參與的每個節點上執行。FPolicy負責建立及維護與外部FPolicy伺服器（FPolicy伺服器）的連線、通知處理、以及管理與FPolicy伺服器之間的通知訊息。

此外、在連線管理中、FPolicy有下列責任：

- 確保檔案通知會透過正確的LIF傳送到FPolicy伺服器。
- 確保當多個FPolicy伺服器與某個原則相關聯時、會在傳送通知給FPolicy伺服器時完成負載平衡。
- 當與FPolicy伺服器的連線中斷時、嘗試重新建立連線。
- 透過驗證的工作階段將通知傳送至FPolicy伺服器。
- 管理FPolicy伺服器所建立的Passthrough-read資料連線、以便在啟用passe-read時、為用戶端要求提供服務。

控制通道如何用於**FPolicy**通訊

FPolicy會從儲存虛擬機器（SVM）上每個節點的資料生命期、啟動與外部FPolicy伺服器的控制通道連線。FPolicy使用控制通道來傳輸檔案通知、因此FPolicy伺服器可能會根據SVM拓撲看到多個控制通道連線。

特殊權限資料存取通道如何用於同步通訊

在同步使用案例中、FPolicy伺服器會透過特殊權限的資料存取路徑、存取儲存虛擬機器（SVM）上的資料。透過權限路徑存取時、會將完整的檔案系統公開給FPolicy伺服器。它可以存取資料檔案來收集資訊、掃描檔案、讀取檔案或寫入檔案。

由於外部FPolicy伺服器可透過特殊權限的資料通道、從SVM的根目錄存取整個檔案系統、因此具有特殊權限的資料通道連線必須安全無虞。

如何將**FPolicy**連線認證用於特殊權限的資料存取通道

FPolicy伺服器會使用與FPolicy組態一起儲存的特定Windows使用者認證、建立與叢集節點的授權資料存取連線。SMB是唯一支援的傳輸協定、可用來建立特殊權限資料存取通道連線。

如果FPolicy伺服器需要存取授權資料、則必須符合下列條件：

- 必須在叢集上啟用SMB授權。
- FPolicy伺服器必須在FPolicy組態中設定的認證下執行。

建立資料通道連線時、FPolicy會使用指定Windows使用者名稱的認證資料。資料存取是透過管理共用ONTAP_admin$進行。

授與超級使用者認證以進行授權資料存取的意義

使用FPolicy組態中設定的IP位址和使用者認證組合、將超級使用者認證授予FPolicy伺服器。ONTAP

當FPolicy伺服器存取資料時、超級使用者狀態會授予下列權限：

- 避免進行權限檢查

  使用者無需檢查檔案和目錄存取。

- 特殊鎖定權限

  支援讀取、寫入或修改任何檔案的存取權限、無論現有的鎖定為何。ONTAP如果FPolicy伺服器對檔案進行位元組範圍鎖定、則會立即移除檔案上現有的鎖定。

- 略過任何FPolicy檢查

  存取不會產生任何FPolicy通知。

FPolicy如何管理原則處理

可能有多個FPolicy原則指派給您的儲存虛擬機器（SVM）、每個原則的優先順序各不相同。若要在SVM上建立適當的FPolicy組態、請務必瞭解FPolicy如何管理原則處理。

每個檔案存取要求都會經過初始評估、以判斷哪些原則正在監控此事件。如果是受監控的事件、則監控事件的相關資訊以及相關的原則都會傳送到FPolicy、並在FPolicy中進行評估。每個原則都會依照指派的優先順序進行評估。

在設定原則時、您應考慮下列建議：

- 當您想要在其他原則之前一律先評估原則時、請以較高的優先順序設定該原則。
- 如果所要求的檔案存取作業在受監控事件上成功、是根據其他原則評估檔案要求的先決條件、請將控制第一個檔案作業成功或失敗的原則設定為較高的優先順序。

  例如、如果一個原則管理FPolicy檔案歸檔與還原功能、而另一個原則管理線上檔案的檔案存取作業、 管理檔案還原的原則必須具有較高的優先順序、才能在第二個原則所管理的作業之前還原檔案。

- 如果您想要評估所有可能套用至檔案存取作業的原則、請將同步原則的優先順序降低。

您可以修改原則順序編號、重新排列現有原則的原則優先順序。不過、若要讓FPolicy根據修改後的優先順序來評估原則、您必須停用並重新啟用具有修改順序編號的原則。

節點到外部 **ONTAP FPolicy** 伺服器通訊過程

若要正確規劃FPolicy組態、您應該瞭解節點對外部FPolicy伺服器的通訊程序為何。

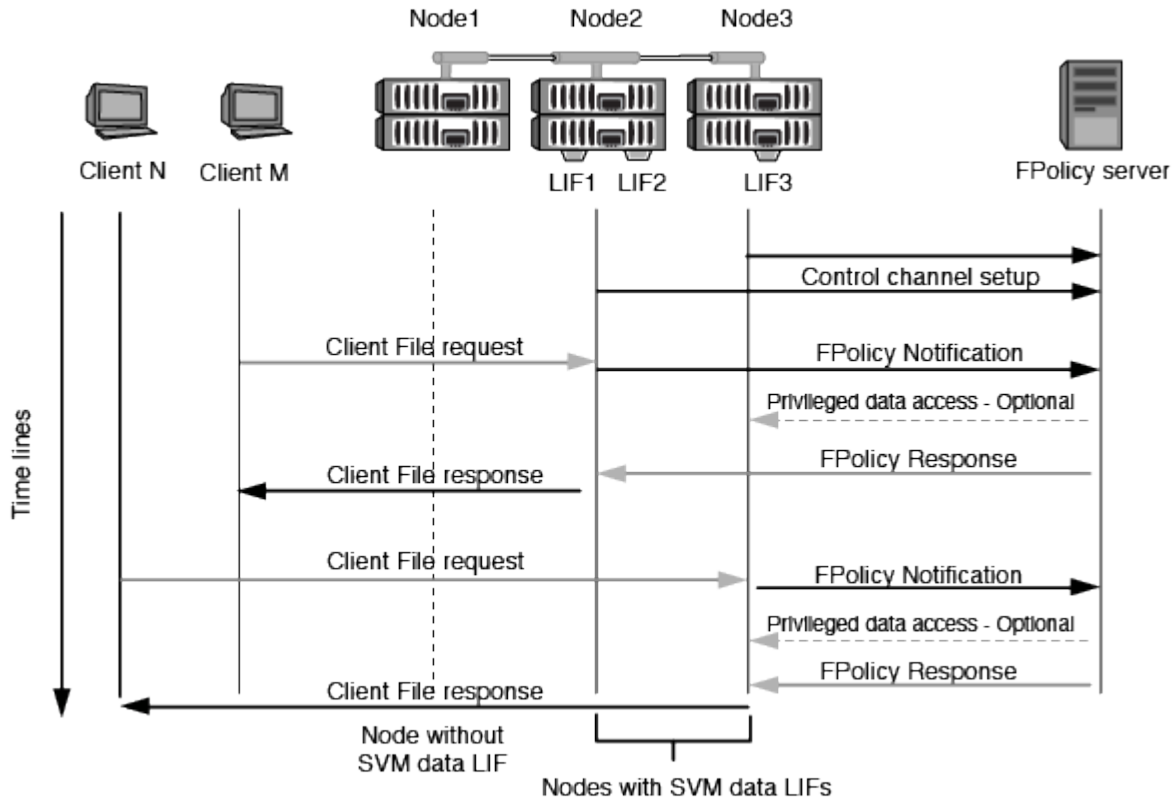
每個參與每個儲存虛擬機器（SVM）的節點、都會使用TCP/IP來啟動與外部FPolicy伺服器（FPolicy伺服器）的連線。與FPolicy伺服器的連線是使用節點資料LIF設定、因此只有當節點具有SVM的作業資料LIF時、參與的節點才能設定連線。

啟用原則時、參與節點上的每個FPolicy程序都會嘗試建立與FPolicy伺服器的連線。它使用原則組態中指定

的FPolicy外部引擎IP位址和連接埠。

此連線會透過資料LIF、從每個SVM上的每個節點建立一個控制通道、以連接至FPolicy伺服器。此外、如果同一個參與節點上有IPV4和IPV6資料LIF位址、FPolicy會嘗試建立連線、以便同時連線至IPV4和IPV6。因此、在SVM延伸到多個節點上的案例中、或是同時存在IPV4和IPV6位址時、FPolicy伺服器必須在SVM上啟用FPolicy原則之後、為叢集的多個控制通道設定要求做好準備。

例如、如果叢集有三個節點（節點1、節點2和節點3）、而SVM資料LIF僅散佈於節點2和節點3、則控制通道只會從節點2和節點3啟動、無論資料磁碟區的分佈為何。說明Node2有兩個屬於SVM的資料生命期、分別是LIF1和LIF2、而且初始連線來自於LIF1。如果LIF1失敗、FPolicy會嘗試從LIF2建立控制通道。



FPolicy如何在LIF移轉或容錯移轉期間管理外部通訊

資料生命期可移轉至同一個節點的資料連接埠、或移轉至遠端節點的資料連接埠。

當資料LIF容錯移轉或移轉時、會建立新的控制通道連線至FPolicy伺服器。然後FPolicy可以重試逾時的SMB和NFS用戶端要求、並將新通知傳送至外部FPolicy伺服器。節點會拒絕FPolicy伺服器對原始、逾時SMB和NFS要求的回應。

FPolicy如何在節點容錯移轉期間管理外部通訊

如果裝載用於FPolicy通訊之資料連接埠的叢集節點故障、ONTAP 則無法中斷FPolicy伺服器與節點之間的連線。

透過設定容錯移轉原則、將 FPolicy 通訊中使用的資料連接埠移轉至另一個作用中節點、可減輕叢集容錯移轉至 FPolicy 伺服器的影響。移轉完成後、會使用新的資料連接埠建立新的連線。

如果未將容錯移轉原則設定為移轉資料連接埠、 FPolicy 伺服器必須等待故障節點啟動。節點啟動後、會使用新

的工作階段ID從該節點啟動新的連線。

FPolicy伺服器會使用「保持作用中」傳輸協定訊息來偵測中斷的連線。清除工作階段ID的逾時是在設定FPolicy時決定。預設的「保持作用中」逾時為兩分鐘。

了解跨 SVM 命名空間的 ONTAP FPolicy 服務

提供統一化儲存虛擬機器（SVM）命名空間。ONTAP叢集內的磁碟區會透過連接點連接在一起、以提供單一的邏輯檔案系統。FPolicy伺服器知道命名空間拓撲、並在命名空間中提供FPolicy服務。

命名空間是特定於SVM並包含在SVM中、因此您只能從SVM內容中查看命名空間。命名空間具有下列特性：

- 每個SVM中都有一個命名空間、命名空間的根目錄為根磁碟區、在命名空間中以斜槓（/）表示。
- 所有其他磁碟區的交會點均低於根（/）。
- Volume交會對用戶端而言是透明的。
- 單一NFS匯出可提供完整命名空間的存取權、否則匯出原則可匯出特定磁碟區。
- SMB共用可在磁碟區或磁碟區內的qtree上建立、或是在命名空間內的任何目錄上建立。
- 命名空間架構具有彈性。

  典型命名空間架構的範例如下：

  - 具有根目錄外單一分支的命名空間
  - 具有多個根目錄分支的命名空間
  - 一個命名空間、其根部有多個未分支的磁碟區

ONTAP FPolicy 直通讀取如何增強分層儲存管理的可用性

Passthsthro-read可讓FPolicy伺服器（做為階層式儲存管理（HSM）伺服器）提供離線檔案的讀取存取權限、而不需要從次要儲存系統將檔案重新叫用至主要儲存系統。

當FPolicy伺服器設定為提供HSM給SMB伺服器上的檔案時、會發生原則型檔案移轉、檔案會離線儲存在次要儲存設備上、而且只有存根檔案保留在主要儲存設備上。雖然存根檔案對用戶端而言是正常檔案、但實際上是與原始檔案大小相同的稀疏檔案。該檔案設有SMB離線位元、並指向已移轉至次要儲存設備的實際檔案。

一般而言、當收到離線檔案的讀取要求時、必須將要求的內容重新叫用回主要儲存設備、然後再透過主要儲存設備存取。需要將資料重新叫用回主儲存設備、會產生幾種不良影響。其中不良的影響包括：回應要求前必須回收內容、導致用戶端要求延遲增加、以及主儲存設備上已回收檔案所需的空間使用量增加。

FPolicy Passthrough-read可讓HSM伺服器（FPolicy伺服器）提供移轉離線檔案的讀取存取權、而不需要從次要儲存系統將檔案重新叫用至主要儲存系統。讀取要求可直接從次要儲存設備處理、而非將檔案重新叫用回主要儲存設備。

FPolicy pass-read作業不支援複本卸載（ODX）。

Passthsther-read提供下列優點、可增強使用性：

- 即使主儲存設備沒有足夠空間可將要求的資料回收回主儲存設備、仍可處理讀取要求。
- 當發生大量的資料回收時（例如指令碼或備份解決方案需要存取許多離線檔案）、容量和效能管理會更好。
- 您可以處理快照中離線檔案的讀取要求。

  由於快照是唯讀的，因此如果存根檔案位於快照中， FPolicy 伺服器就無法還原原始檔案。使用Passthrough-read可消除此問題。

- 您可以設定原則、以控制何時透過存取次要儲存設備上的檔案來處理讀取要求、以及何時應將離線檔案重新叫用至主要儲存設備。

  例如、您可以在HSM伺服器上建立原則、指定在檔案移轉回主要儲存設備之前、於指定時間段內存取離線檔案的次數。這類原則可避免重呼很少存取的檔案。

啟用**FPolicy Passthrough-read**時、如何管理讀取要求

您應該瞭解啟用FPolicy pass-read時如何管理讀取要求、以便最佳設定儲存虛擬機器（SVM）與FPolicy伺服器之間的連線。

啟用FPolicy Passthrough-read且SVM收到離線檔案的要求時、FPolicy會透過標準連線通道傳送通知給FPolicy伺服器（HSM伺服器）。

收到通知後、FPolicy伺服器會從通知中傳送的檔案路徑讀取資料、並透過SVM與FPolicy伺服器之間建立的Passthrough-read權限資料連線、將要求的資料傳送至SVM。

傳送資料後、FPolicy伺服器會以允許或拒絕的形式回應讀取要求。根據讀取要求是允許還是拒絕、ONTAP 所以無法傳送要求的資訊或傳送錯誤訊息給用戶端。

版權資訊

商標資訊