在SVM上使用FPolicy進行檔案監控與管理

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/ontap/nas-audit/two-parts-fpolicy-solution-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

目錄

在SVM上使用FPolicy進行檔案監控與管理 1
瞭解 FPolicy 1
規劃FPolicy組態 9
建立FPolicy組態 39
管理 FPolicy 組態 46

在SVM上使用FPolicy進行檔案監控與管理

瞭解 FPolicy

FPolicy解決方案的兩個部分是什麼

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和 NetApp 產品工作負載安全性和雲端資料感知。

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。

什麼是同步和非同步通知

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

FPolicy 永續性儲存區

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。

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。

最佳實務做法

叢集管理員必須在啟用 FPolicy 的每個 SVM 上、為持續儲存區設定磁碟區。設定後、持續儲存區會擷取所有符合的 FPolicy 事件、這些事件會在 FPolicy 管道中進一步處理、並傳送至外部伺服器。

當發生非預期的重新開機或停用 FPolicy 並再次啟用時、持續儲存區仍會保持上次收到事件的狀態。在接管作業之後、新事件將會由合作夥伴節點儲存及處理。恢復作業完成後、持續儲存區會繼續處理任何未處理的事件、這些事件可能會在節點接管發生時保留。即時事件將優先於未處理的事件。

如果持續儲存區磁碟區在同一個 SVM 中從一個節點移至另一個節點、則尚未處理的通知也會移至新節點。您需要重新執行 `fpolicy persistent-store create` 在磁碟區移動之後、在任一節點上執行命令、以確保擱置的通知會傳送至外部伺服器。

持續儲存區 Volume 是以每個 SVM 為基礎進行設定。對於每個啟用 FPolicy 的 SVM 、您都需要建立持續儲存區 Volume 。

在具有預期由 Fpolicy 監控最大流量的生命期的節點上建立持續儲存區磁碟區。

如果持續儲存區中累積的通知超過已配置的磁碟區大小、 FPolicy 將開始丟棄傳入通知、並顯示適當的 EMS 訊息。

在建立磁碟區時指定的持續儲存區磁碟區名稱和交會路徑應相符。

將 Snapshot 原則設為 `none` 而非 `default`。這是為了確保不會意外還原快照而導致目前事件遺失、並防止可能的重複事件處理。

讓外部使用者傳輸協定存取（ CIFS/NFS ）無法存取持續儲存區磁碟區、以避免意外毀損或刪除持續存在的事件記錄。為達成此目的、在啟用 FPolicy 之後、請在 ONTAP 中卸載磁碟區以移除連接路徑、這會使使用者傳輸協定存取無法存取。

如需詳細資訊、請參閱 "建立持續儲存區"。

FPolicy組態類型

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。

叢集元件在**FPolicy**實作中扮演的角色

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。

FPolicy如何搭配外部**FPolicy**伺服器運作

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。

節點對外部**FPolicy**伺服器的通訊程序為何

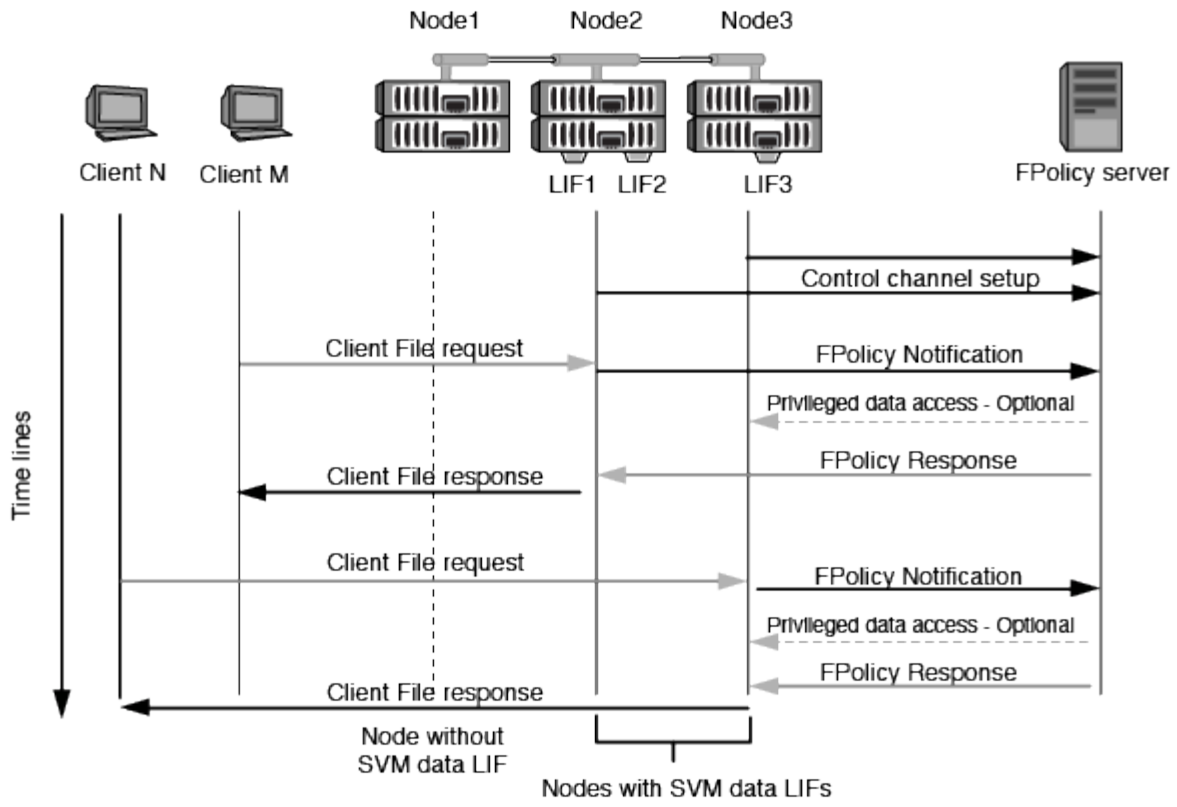
若要正確規劃FPolicy組態、您應該瞭解節點對外部FPolicy伺服器的通訊程序為何。

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。

FPolicy服務如何跨**SVM**命名空間運作

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

FPolicy Passthrough-read如何強化階層式儲存管理的使用性

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。
- Snapshot複本中離線檔案的讀取要求可以提供服務。

  由於Snapshot複本為唯讀、因此如果存根檔案位於Snapshot複本中、FPolicy伺服器將無法還原原始檔案。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。

規劃**FPolicy**組態

設定**FPolicy**的需求、考量及最佳實務做法

在SVM上建立及設定FPolicy組態之前、您必須先瞭解設定FPolicy的特定需求、考量事項及最佳實務做法。

FPolicy 功能可透過命令列介面（ CLI ）或 REST API 進行設定。

設定**FPolicy**的需求

在儲存虛擬機器（SVM）上設定及啟用FPolicy之前、您必須先瞭解特定需求。

- 叢集中的所有節點都必須執行ONTAP 支援FPolicy的版本的功能。
- 如果您不使用ONTAP 本機的FPolicy引擎、則必須安裝外部FPolicy伺服器（FPolicy伺服器）。
- FPolicy伺服器必須安裝在可從啟用FPolicy原則的SVM資料生命區存取的伺服器上。

> 從Sf9.8開始ONTAP 、ONTAP 這個解決方案提供用戶端LIF服務、可用於新增的輸出FPolicy連線 `data-fpolicy-client` 服務： "深入瞭解生命與服務原則"。

- FPolicy伺服器的IP位址必須在FPolicy原則外部引擎組態中設定為主要或次要伺服器。
- 如果FPolicy伺服器透過特殊權限的資料通道存取資料、則必須滿足下列額外需求：
  - SMB必須在叢集上獲得授權。

    特殊權限資料存取是使用SMB連線來完成。
  - 必須設定使用者認證、才能透過權限資料通道存取檔案。
  - FPolicy伺服器必須在FPolicy組態中設定的認證下執行。
  - 用於與 FPolicy 伺服器通訊的所有資料生命都必須設定為具有 `cifs` 作為其中一種允許的通訊協定。

    這包括用於傳遞讀取連線的lifs。

- 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。

設定**FPolicy**時的最佳實務做法與建議

在儲存虛擬機器（SVM）上設定 FPolicy 時、請熟悉一般組態最佳實務做法和建議、以確保 FPolicy 組態能提供強大的監控效能和符合您需求的結果。

如需效能、規模調整及組態的特定準則、請與 FPolicy 合作夥伴應用程式合作。

原則組態

設定 FPolicy 外部引擎、事件和 SVM 範圍、可改善您的整體體驗和安全性。

- 設定 SVM 的 FPolicy 外部引擎：
  - 提供額外的安全性需要付出效能成本。啟用安全通訊端層（SSL）通訊對存取共用具有效能影響。
  - FPolicy 外部引擎應設定多個 FPolicy 伺服器、以提供 FPolicy 伺服器通知處理的恢復能力和高可用度。
- 設定 SVM 的 FPolicy 事件：

  監控檔案作業會影響您的整體體驗。例如、在儲存端篩選不想要的檔案作業、可改善您的使用體驗。NetApp 建議設定下列組態：

  - 監控檔案作業的最小類型、並在不中斷使用案例的情況下啟用最大篩選器數量。
  - 使用篩選器執行 getattr 、讀取、寫入、開啟及關閉作業。SMB 和 NFS 主目錄環境在這些作業中所佔的比例很高。
- SVM 的 FPolicy 範圍組態：

  將原則的範圍限制在相關的儲存物件上、例如共用、磁碟區和匯出、而非在整個 SVM 中啟用這些物件。NetApp 建議您檢查目錄副檔名。如果是 `is-file-extension-check-on-directories-enabled` 參數設定為 `true`，目錄物件會受到與一般檔案相同的副檔名檢查。

網路組態

FPolicy 伺服器與控制器之間的網路連線應為低延遲。NetApp 建議使用私有網路來分隔 FPolicy 流量與用戶端流量。

此外、您應該將外部 FPolicy 伺服器（FPolicy 伺服器）放置在離具有高頻寬連線能力的叢集近的位置、以提供最小的延遲和高頻寬連線能力。

> 如果將 FPolicy 流量的 LIF 設定在與 LIF 不同的連接埠上、以進行用戶端流量、則 FPolicy LIF 可能會因為連接埠故障而容錯移轉至其他節點。因此、 FPolicy 伺服器無法從節點連線、導致 FPolicy 通知節點上的檔案作業失敗。若要避免此問題、請確認可透過節點上至少一個 LIF 來連線 FPolicy 伺服器、以處理在該節點上執行檔案作業的 FPolicy 要求。

硬體組態

您可以在實體伺服器或虛擬伺服器上使用 FPolicy 伺服器。如果 FPolicy 伺服器位於虛擬環境中、您應該將專用資源（CPU 、網路和記憶體）分配給虛擬伺服器。

叢集節點對FPolicy伺服器比率應最佳化、以確保FPolicy伺服器不會過載、這可能會在SVM回應用戶端要求時產生延遲。最佳比率取決於使用 FPolicy 伺服器的合作夥伴應用程式。NetApp 建議與合作夥伴合作、以確定適當的價值。

多原則組態

無論序號為何、原生封鎖的 FPolicy 原則都具有最高優先順序、而變更決策原則的優先順序比其他原則高。原則優先順序取決於使用案例。NetApp 建議與合作夥伴合作、以決定適當的優先順序。

規模考量

FPolicy 會執行 SMB 和 NFS 作業的即時監控、傳送通知給外部伺服器、並根據外部引擎通訊模式（同步或非同步）等待回應。此程序會影響 SMB 和 NFS 存取和 CPU 資源的效能。

為了減輕任何問題、 NetApp 建議您在啟用 FPolicy 之前、先與合作夥伴合作、評估環境並調整其規模。效能受到多種因素影響、包括使用者數量、工作負載特性、例如每位使用者的作業次數和資料大小、網路延遲、故障或伺服器速度緩慢。

監控效能

FPolicy 是以通知為基礎的系統。通知會傳送至外部伺服器以進行處理、並產生回覆 ONTAP 的回應。此往返程序會增加用戶端存取的延遲。

監控 FPolicy 伺服器和 ONTAP 中的效能計數器、可讓您識別解決方案中的瓶頸、並視需要調整參數、以獲得最佳解決方案。例如、 FPolicy 延遲增加會對 SMB 和 NFS 存取延遲造成串聯影響。因此、您應該同時監控工作負載（ SMB 和 NFS ）和 FPolicy 延遲。此外、您可以在 ONTAP 中使用服務品質原則、為每個啟用 FPolicy 的 Volume 或 SVM 設定工作負載。

NetApp 建議您執行 `statistics show -object workload` 顯示工作負載統計資料的命令。此外、您應該監控下列參數：

- 平均、讀取和寫入延遲
- 作業總數
- 讀寫計數器

您可以使用下列 FPolicy 計數器來監控 FPolicy 子系統的效能。

> 您必須處於診斷模式、才能收集與 FPolicy 相關的統計資料。

步驟

1. 收集 FPolicy 計數器：
   a. `statistics start -object fpolicy -instance` *`instance_name`* `-sample-id` *`ID`*
   b. `statistics start -object fpolicy_policy -instance` *`instance_name`* `-sample-id` *`ID`*
2. 顯示 FPolicy 計數器：
   a. `statistics show -object fpolicy -instance` *`instance_name`* `-sample-id` *`ID`*
   b. `statistics show -object fpolicy_server -instance` *`instance_name`* `-sample-id` *`ID`*

- `fpolicy` 和 `fpolicy_server` Counters 提供下表所述數種效能參數的相關資訊。

計數器	說明
• 「 fpolicy 」計數器 *	aborted_requests
在 SVM 上中止處理的畫面要求數	event_count
導致通知的事件清單	max_requent_l滯
最大螢幕要求延遲時間	未處理的要求
處理中的畫面要求總數	Processed_requests
在 SVM 上執行 fpolicy 處理的畫面要求總數	requy_histure_hist
畫面要求延遲長條圖	Requests_Dispatched_Rate
每秒發出的畫面要求數	Requests_receiped_rate
每秒接收的畫面要求數	• 「 fpolicy_server 」計數器 *
max_requent_l滯	畫面要求的最大延遲
未處理的要求	等待回應的畫面要求總數
requy_l滯	畫面要求的平均延遲
requy_histure_hist	畫面要求延遲長條圖
requy_sent_rate	每秒傳送至 FPolicy 伺服器的畫面要求數
RESPONY_REATE_RATE	每秒從 FPolicy 伺服器收到的畫面回應數

管理 **FPolicy** 工作流程、並仰賴其他技術

NetApp 建議您先停用 FPolicy 原則、再進行任何組態變更。例如、如果您想要新增或修改為啟用原則設定的外部引擎中的 IP 位址、請先停用原則。

如果您將 FPolicy 設定為監控 NetApp FlexCache 磁碟區、 NetApp 建議您不要設定 FPolicy 來監控讀取和 getattr 檔案作業。在 ONTAP 中監控這些作業需要擷取 inode 到路徑 （ I2P ） 資料。由於 I2P 資料無法從 FlexCache 磁碟區擷取、因此必須從原始磁碟區擷取。因此、監控這些作業可免除 FlexCache 所能提供的效能效益。

當同時部署 FPolicy 和隨裝即用的防毒解決方案時、防毒解決方案會先收到通知。FPolicy 處理只會在防毒掃描完成後才會開始。請務必正確設定防毒解決方案的大小、因為慢速防毒掃描程式可能會影響整體效能。

Passthsther-read升級與還原考量

在升級ONTAP 至支援Passthrough-read的版本之前、或在回復至不支援passe-read的版本之前、您必須瞭解某些升級與還原考量事項。

升級

將所有節點升級至ONTAP 支援FPolicy Passthrough-read的版本後、叢集就能使用Passthrough-read功能；不過、在現有的FPolicy組態上、依預設會停用pass-read。若要在現有的FPolicy組態上使用passThrough讀取、您必須停用FPolicy原則並修改組態、然後重新啟用組態。

還原

還原至不支援 FPolicy Passthrough-read 的 ONTAP 版本之前、您必須符合下列條件：

- 使用 Passthrough-read 停用所有原則、然後修改受影響的組態、使其不使用 passthrough Read 。
- 停用叢集上的每個 FPolicy 原則、以停用叢集上的 FPolicy 功能。

在還原至不支援持續儲存區的 ONTAP 版本之前、請先確定所有 Fpolicy 原則都沒有設定的持續儲存區。如果設定持續儲存區、還原將會失敗。

設定**FPolicy**組態的步驟為何

在FPolicy能夠監控檔案存取之前、必須先在需要FPolicy服務的儲存虛擬機器（SVM）上建立並啟用FPolicy組態。

在SVM上設定及啟用FPolicy組態的步驟如下：

1. 建立FPolicy外部引擎。

   FPolicy外部引擎可識別與特定FPolicy組態相關聯的外部FPolicy伺服器（FPolicy伺服器）。如果使用內部的「原生」FPolicy引擎來建立原生檔案封鎖組態、則不需要建立FPolicy外部引擎。

2. 建立FPolicy事件。

   FPolicy事件說明FPolicy原則應監控的項目。事件包括要監控的傳輸協定和檔案作業、並可包含篩選器清單。事件使用篩選器來縮小FPolicy外部引擎必須傳送通知的受監控事件清單。事件也會指定原則是否監控Volume作業。

3. 建立FPolicy原則。

   FPolicy原則負責將需要監控的一組事件與適當範圍相關聯、以及哪些受監控的事件通知必須傳送至指定的FPolicy伺服器（若未設定FPolicy伺服器、則會傳送至原生引擎）。該原則也定義是否允許FPolicy伺服器以權限存取其接收通知的資料。如果伺服器需要存取資料、FPolicy伺服器就需要存取權限。需要存取權限的典型使用案例包括檔案封鎖、配額管理及階層式儲存管理。您可以在原則中指定此原則的組態是使用FPolicy伺服器、還是使用內部的「原生」FPolicy伺服器。

   原則會指定是否必須篩選。如果篩選是強制性的、且所有FPolicy伺服器都關閉、或在定義的逾時期間內、未從FPolicy伺服器收到任何回應、則檔案存取將遭拒。

   原則的界限是SVM。原則無法套用至多個SVM。不過、特定SVM可以有多個FPolicy原則、每個原則的範圍、事件和外部伺服器組態組合相同或不同。

4. 設定原則範圍。

   FPolicy範圍決定原則在哪些磁碟區、共享區或匯出原則上執行、或排除在監控範圍之外。範圍也會決定哪些副檔名應納入或排除在FPolicy監控範圍之外。

排除清單優先於包含清單。

5. 啟用FPolicy原則。

   啟用原則時、會連接控制通道和（可選）特殊權限資料通道。SVM參與之節點上的FPolicy程序會開始監控檔案和資料夾存取、若事件符合設定的條件、則會將通知傳送至FPolicy伺服器（若未設定FPolicy伺服器、則會傳送至原生引擎）。

   如果原則使用原生檔案封鎖、則不會設定外部引擎、也不會與原則建立關聯。

規劃**FPolicy**外部引擎組態

規劃**FPolicy**外部引擎組態

在設定FPolicy外部引擎（外部引擎）之前、您必須先瞭解建立外部引擎的意義、以及可用的組態參數。此資訊可協助您判斷要為每個參數設定哪些值。

建立**FPolicy**外部引擎時所定義的資訊

外部引擎組態定義FPolicy建立及管理外部FPolicy伺服器（FPolicy伺服器）連線所需的資訊、包括下列資訊：

- SVM名稱
- 引擎名稱
- 主要和次要FPolicy伺服器的IP位址、以及連接至FPolicy伺服器時要使用的TCP連接埠號碼
- 引擎類型為非同步或同步
- 如何驗證節點與FPolicy伺服器之間的連線

  如果您選擇設定相互SSL驗證、則也必須設定提供SSL憑證資訊的參數。

- 如何使用各種進階權限設定來管理連線

  這包括定義逾時值、重試值、保持活動值、最大要求值、傳送和接收緩衝區大小值、以及工作階段逾時值等項目的參數。

。`vserver fpolicy policy external-engine create` 命令用於建立 FPolicy 外部引擎。

基本的外部引擎參數是什麼

您可以使用下表的基本FPolicy組態參數來協助規劃組態：

資訊類型	選項

SVM 指定您要與此外部引擎建立關聯的SVM名稱。 每個FPolicy組態都是在單一SVM中定義。為了建立FPolicy原則組態、而將外部引擎、原則事件、原則範圍和原則結合在一起的原則、都必須與相同的SVM建立關聯。	`-vserver vserver_name`
引擎名稱_ 指定要指派給外部引擎組態的名稱。之後建立FPolicy原則時、您必須指定外部引擎名稱。這會將外部引擎與原則建立關聯。 名稱最長可達256個字元。 ⓘ 如果在MetroCluster 一個還原或SVM災難恢復組態中設定外部引擎名稱、名稱最長應為200個字元。 名稱可以包含下列任何Ascii範圍字元的組合： • `a` 透過 `z` • `A` 透過 `Z` • `0` 透過 `9` • “_” 、 “-”, and “.”	`-engine-name engine_name`
主要*FPolicy*伺服器 指定節點傳送特定FPolicy原則通知的主要FPolicy伺服器。此值會指定為以逗號分隔的IP位址清單。 如果指定多個主要伺服器IP位址、則SVM參與的每個節點都會在原則啟用時、建立每個指定主要FPolicy伺服器的控制連線。如果您設定多個主要FPolicy伺服器、通知會以循環配置資源的方式傳送至FPolicy伺服器。 如果外部引擎用於MetroCluster SVM災難恢復組態、您應該將來源站台FPolicy伺服器的IP位址指定為主要伺服器。目的地站台FPolicy伺服器的IP位址應指定為次要伺服器。	`-primary-servers IP_address`、 …
連接埠號碼_ 指定FPolicy服務的連接埠號碼。	`-port integer`

次要FPolicy伺服器_ 指定次要FPolicy伺服器、以便針對指定的FPolicy原則傳送檔案存取事件。此值會指定為以逗號分隔的IP位址清單。 次要伺服器只會在無法連線到任何一部主要伺服器時使用。當原則啟用時、就會建立次要伺服器的連線、但只有在所有主要伺服器都無法連線時、才會將通知傳送到次要伺服器。如果您設定多個次要伺服器、通知會以循環配置資源的方式傳送至FPolicy伺服器。	`-secondary-servers IP_address`、 ...
外部引擎類型_ 指定外部引擎是以同步或非同步模式運作。根據預設、FPolicy會以同步模式運作。 設定為時 `synchronous`、檔案要求處理會傳送通知給 FPolicy 伺服器、但在收到 FPolicy 伺服器的回應之後才會繼續。此時、視FPolicy伺服器的回應是否允許要求的動作而定、要求流程會繼續或處理會導致拒絕。 設定為時 `asynchronous`、檔案要求處理會傳送通知給 FPolicy 伺服器、然後繼續。	`-extern-engine-type external_engine_type` 此參數的值可以是下列其中一項： • `synchronous` • `asynchronous`
與FPolicy server_通訊的_SSL選項 指定與FPolicy伺服器通訊的SSL選項。這是必要的參數。您可以根據下列資訊選擇其中一個選項： • 設定為時 `no-auth`、不進行驗證。 通訊連結是透過TCP建立。 • 設定為時 `server-auth`， SVM 使用 SSL 伺服器驗證來驗證 FPolicy 伺服器。 • 設定為時 `mutual-auth`、在 SVM 和 FPolicy 伺服器之間進行相互驗證； SVM 驗證 FPolicy 伺服器、 FPolicy 伺服器驗證 SVM 。 如果您選擇設定相互 SSL 驗證、則也必須設定 `-certificate -common-name`、 `-certificate-serial`和 `-certifcate-ca` 參數。	`-ssl-option` {`no-auth`
`server-auth`	`mutual-auth`}
憑證*FQDN*或自訂通用名稱 指定在SVM與FPolicy伺服器之間設定SSL驗證時所使用的憑證名稱。您可以將憑證名稱指定為FQDN或自訂通用名稱。 如果您指定 `mutual-auth` 適用於 `-ssl-option` 參數、您必須指定的值 `-certificate-common-name` 參數。	`-certificate-common -name text`

憑證序號 指定在SVM與FPolicy伺服器之間設定SSL驗證時、用於驗證的憑證序號。 如果您指定 `mutual-auth` 適用於 `-ssl-option` 參數、您必須指定的值 `-certificate-serial` 參數。	`-certificate-serial text`
憑證授權單位 指定在SVM與FPolicy伺服器之間設定SSL驗證時、用於驗證的憑證CA名稱。 如果您指定 `mutual-auth` 適用於 `-ssl-option` 參數、您必須指定的值 `-certificate-ca` 參數。	`-certificate-ca text`

進階的外部引擎選項是什麼

您可以在規劃是否使用進階參數自訂組態時、使用下表的進階FPolicy組態參數。您可以使用這些參數來修改叢集節點與FPolicy伺服器之間的通訊行為：

資訊類型	選項
取消要求的逾時_ 指定時間間隔（小時）（`h`）、分鐘 (`m`）或秒 (`s`）節點等待 FPolicy 伺服器的回應。 如果逾時時間間隔超過、節點會將取消要求傳送至FPolicy伺服器。然後、節點會將通知傳送至替代的FPolicy伺服器。此逾時有助於處理無回應的FPolicy伺服器、進而改善SMB/NFS用戶端回應。此外、在逾時期間之後取消要求、也有助於釋出系統資源、因為通知要求會從停機/不良的FPolicy伺服器移至替代的FPolicy伺服器。 此值的範圍為 `0` 透過 `100`。如果值設為 `0`，此選項已停用，取消要求訊息不會傳送至 FPolicy 伺服器。預設值為 `20s`。	`-reqs-cancel-timeout integer`[h
m	s]
中止要求的逾時_ 指定逾時（以小時為單位）（`h`）、分鐘 (`m`）或秒 (`s`）以中止要求。 此值的範圍為 `0` 透過 `200`。	`-reqs-abort-timeout` ` `integer`[h
m	s]

傳送狀態要求的時間間隔 指定以小時為單位的時間間隔 (h）、分鐘 (m）或秒 (s）之後、狀態要求會傳送至 FPolicy 伺服器。 此值的範圍為 0 透過 50。如果值設為 0、選項已停用、狀態要求訊息不會傳送至 FPolicy 伺服器。預設值為 10s。	-status-req-interval integer[h
m	s]
*FPolicy*伺服器上未處理的要求上限 指定可在FPolicy伺服器上排入佇列的未處理要求數目上限。 此值的範圍為 1 透過 10000。預設值為 500。	-max-server-reqs integer
中斷無回應的*FPolicy*伺服器連線逾時 指定時間間隔（小時）（h）、分鐘 (m）或秒 (s）之後、會終止與 FPolicy 伺服器的連線。 只有FPolicy伺服器的佇列包含允許的最大要求數、且在逾時期間內未收到任何回應時、才會在逾時期間之後終止連線。允許的最大要求數為其中之一 50（預設）或指定的號碼 max-server-reqs- 參數。 此值的範圍為 1 透過 100。預設值為 60s。	-server-progress -timeout integer[h
m	s]
_將保持活動訊息傳送至FPolicy server_的時間間隔 指定時間間隔（小時）（h）、分鐘 (m）或秒 (s）將保持活動的訊息傳送到 FPolicy 伺服器。 「保持連線」訊息會偵測半開啟的連線。 此值的範圍為 10 透過 600。如果值設為 0，此選項會停用，並防止將持續作用的訊息傳送至 FPolicy 伺服器。預設值為 120s。	-keep-alive-interval-integer[h
m	s]
最大重新連線嘗試次數_ 指定SVM在連線中斷後嘗試重新連線至FPolicy伺服器的最大次數。 此值的範圍為 0 透過 20。預設值為 5。	-max-connection-retries integer

接收緩衝區大小_ 指定FPolicy伺服器之連接插槽的接收緩衝區大小。 預設值設為256 KB。當值設定為0時、接收緩衝區的大小會設定為系統定義的值。 例如、如果套接字的預設接收緩衝區大小為65536位元組、將可調值設為0、則套接字緩衝區大小會設為65536位元組。您可以使用任何非預設值來設定接收緩衝區的大小（以位元組為單位）。	`-recv-buffer-size integer`
傳送緩衝區大小 指定FPolicy伺服器之連線通訊端的傳送緩衝區大小。 預設值設為256 KB。當值設定為0時、傳送緩衝區的大小會設定為系統定義的值。 例如、如果套接字的預設傳送緩衝區大小設為65536位元組、將可調值設為0、則套接字緩衝區大小會設為65536位元組。您可以使用任何非預設值來設定傳送緩衝區的大小（以位元組為單位）。	`-send-buffer-size integer`
重新連線期間清除工作階段*ID*逾時 指定以小時為單位的時間間隔 (`h`）、分鐘 (`m`）或秒 (`s`）之後、新的工作階段 ID 會在重新連線嘗試期間傳送至 FPolicy 伺服器。 如果儲存控制器與FPolicy伺服器之間的連線終止、並在中進行重新連線 `-session-timeout` 時間間隔時、舊的工作階段ID會傳送至FPolicy伺服器、以便傳送舊通知的回應。 預設值設為 10 秒。	`-session-timeout [integerh][integerM][integers]`

設定**FPolicy**外部引擎使用**SSL**驗證連線的其他相關資訊

如果您想要設定FPolicy外部引擎、以便在連線至FPolicy伺服器時使用SSL、您需要知道一些其他資訊。

SSL伺服器驗證

如果您選擇將FPolicy外部引擎設定為SSL伺服器驗證、則在建立外部引擎之前、必須先安裝簽署FPolicy伺服器憑證的憑證授權單位（CA）的公開憑證。

相互驗證

如果您將FPolicy外部引擎設定為在將儲存虛擬機器（SVM）資料LIF連線至外部FPolicy伺服器時使用SSL相互驗證、則在建立外部引擎之前、 您必須安裝簽署FPolicy伺服器憑證的CA公開憑證、以及用於驗證SVM的公開憑證和金鑰檔。當任何FPolicy原則使用已安裝的憑證時、您不得刪除此憑證。

如果在FPolicy連線至外部FPolicy伺服器時、憑證被刪除、則無法重新啟用使用該憑證的停用FPolicy原則。在這

種情況下、即使在SVM上建立並安裝了具有相同設定的新憑證、也無法重新啟用FPolicy原則。

如果憑證已刪除、您需要安裝新的憑證、建立使用新憑證的新FPolicy外部引擎、並透過修改FPolicy原則、將新的外部引擎與您要重新啟用的FPolicy原則建立關聯。

安裝**SSL**憑證

用來簽署 FPolicy 伺服器憑證的 CA 公用憑證是使用安裝 `security certificate install` 命令 `-type` 參數設為 `client-ca`。使用安裝驗證 SVM 所需的私密金鑰和公開憑證 `security certificate install` 命令 `-type` 參數設為 `server`。

憑證無法在**SVM**災難恢復關係中複寫非**ID**保留組態

連線至FPolicy伺服器時用於SSL驗證的安全性憑證、不會以非ID-preserve組態複寫至SVM災難恢復目的地。雖然已複寫SVM上的FPolicy外部引擎組態、但不會複寫安全性憑證。您必須在目的地上手動安裝安全性憑證。

當您設定 SVM 災難恢復關係時、您為選取的值 `-identity-preserve` 的選項 `snapmirror create` 命令可決定在目的地 SVM 中複寫的組態詳細資料。

如果您設定 `-identity-preserve` 選項 `true` （ ID-preserve ）、所有 FPolicy 組態詳細資料都會複寫、包括安全性憑證資訊。只有當您將選項設定為時、才必須在目的地上安裝安全性憑證 `false` （非 ID-Preserve ）。

叢集範圍內的**FPolicy**外部引擎、搭配**MetroCluster** 使用功能性和**SVM**災難恢復組態的限制

您可以將叢集儲存虛擬機器（SVM）指派給外部引擎、藉此建立叢集範圍內的FPolicy外部引擎。然而、在MetroCluster 使用叢集或SVM災難恢復組態建立以叢集為範圍的外部引擎時、選擇SVM用於與FPolicy伺服器進行外部通訊的驗證方法時、會有某些限制。

建立外部FPolicy伺服器時、您可以選擇三種驗證選項：無驗證、SSL伺服器驗證和SSL相互驗證。雖然在選擇驗證選項時沒有任何限制、但如果將外部FPolicy伺服器指派給資料SVM、則在建立叢集範圍的FPolicy外部引擎時仍有限制：

組態	是否允許？
不含驗證的SVM災難恢復和叢集範圍的FPolicy外部引擎（未設定SSL ）MetroCluster	是的
包含SSL伺服器或SSL相互驗證的SVM災難恢復、以及叢集範圍的FPolicy外部引擎MetroCluster	否

- 如果存在具有SSL驗證的叢集範圍FPolicy外部引擎、而您想要建立MetroCluster 一套支援還原或SVM災難恢復的組態、您必須先修改此外部引擎、使其不使用驗證、或是移除外部引擎、才能建立MetroCluster 還原或SVM災難恢復組態。
- 如果MetroCluster 已存在支援功能的不支援功能或SVM災難恢復組態、ONTAP 則無法使用SSL驗證來建立叢集範圍的FPolicy外部引擎。

完成**FPolicy**外部引擎組態工作表

您可以使用這份工作表來記錄FPolicy外部引擎組態程序期間所需的值。如果需要參數值、您必須先判斷這些參數的使用值、再設定外部引擎。

基本外部引擎組態資訊

您應該記錄是否要在外部引擎組態中包含每個參數設定、然後記錄您要納入的參數值。

資訊類型	必要	包括	您的價值
儲存虛擬機器（SVM）名稱	是的	是的	
引擎名稱	是的	是的	
主要FPolicy伺服器	是的	是的	
連接埠號碼	是的	是的	
次要FPolicy伺服器	否		
外部引擎類型	否		
用於與外部FPolicy伺服器通訊的SSL選項	是的	是的	
憑證FQDN或自訂通用名稱	否		
憑證序號	否		
憑證授權單位	否		

進階外部引擎參數資訊

若要使用進階參數設定外部引擎、您必須在進階權限模式下輸入組態命令。

資訊類型	必要	包括	您的價值
取消要求逾時	否		
中止要求的逾時	否		
傳送狀態要求的時間間隔	否		
FPolicy伺服器上未處理的要求上限	否		

中斷無回應的FPolicy伺服器連線逾時	否		
將「保持作用中」訊息傳送至FPolicy伺服器的時間間隔	否		
最大重新連線嘗試次數	否		
接收緩衝區大小	否		
傳送緩衝區大小	否		
重新連線期間清除工作階段ID的逾時	否		

規劃**FPolicy**事件組態

規劃**FPolicy**事件組態總覽

在設定FPolicy事件之前、您必須先瞭解建立FPolicy事件的意義。您必須決定要監控事件的傳輸協定、要監控的事件、以及要使用的事件篩選器。此資訊可協助您規劃要設定的值。

建立**FPolicy**事件的意義

建立FPolicy事件是指定義FPolicy程序所需的資訊、以決定要監控的檔案存取作業、以及應將哪些受監控事件通知傳送至外部FPolicy伺服器。FPolicy事件組態定義下列組態資訊：

- 儲存虛擬機器（SVM）名稱
- 事件名稱
- 要監控的傳輸協定

  FPolicy可以監控SMB、NFSv3和NFSv4檔案存取作業。

- 要監控的檔案作業

  並非所有檔案作業都適用於每個傳輸協定。

- 要設定哪些檔案篩選器

  只有特定的檔案作業與篩選組合有效。每個傳輸協定都有自己的一組支援組合。

- 是否要監控磁碟區掛載和卸載作業

其中三個參數有相依性 (`-protocol`、 `-file-operations`、 `-filters`）。下列組合對三個參數有效：

- 您可以指定 `-protocol` 和 `-file-operations` 參數。
- 您可以指定全部三個參數。
- 您不能指定任何參數。

FPolicy事件組態包含的內容

您可以使用下列可用的FPolicy事件組態參數清單來協助規劃組態：

資訊類型	選項
SVM 指定您要與此FPolicy事件相關聯的SVM名稱。 每個FPolicy組態都是在單一SVM中定義。為了建立FPolicy原則組態、而將外部引擎、原則事件、原則範圍和原則結合在一起的原則、都必須與相同的SVM建立關聯。	`-vserver vserver_name`
事件名稱_ 指定要指派給FPolicy事件的名稱。當您建立FPolicy原則時、會使用事件名稱將FPolicy事件與原則建立關聯。 名稱最長可達256個字元。 如果在MetroCluster 還原或SVM災難恢復組態中設定事件、名稱最長應為200個字元。 名稱可以包含下列任何Ascii範圍字元的組合： • `a` 透過 `z` • `A` 透過 `Z` • `0` 透過 `9` • "_" 、 "-`", and “.”	`-event-name event_name`

傳輸協定 指定要為FPolicy事件設定的傳輸協定。的清單 `-protocol` 可以包含下列其中一個值： • `cifs` • `nfsv3` • `nfsv4` 如果您指定 `-protocol`、然後您必須在中指定有效值 `-file-operations` 參數。隨著傳輸協定版本變更、有效值可能會變更。	`-protocol protocol`
_File operations _ 指定FPolicy事件的檔案作業清單。 事件會使用中指定的通訊協定、從所有用戶端要求檢查此清單中指定的作業 `-protocol` 參數。您可以使用以逗號分隔的清單來列出一或多個檔案作業。的清單 `-file-operations` 可以包含下列一或多個值： • `close` 用於檔案關閉作業 • `create` 用於檔案建立作業 • `create-dir` 用於目錄建立作業 • `delete` 用於檔案刪除作業 • `delete_dir` 用於目錄刪除作業 • `getattr` 以取得屬性作業 • `link` 用於連結作業 • `lookup` 用於查詢作業 • `open` 適用於檔案開啟作業 • `read` 檔案讀取作業 • `write` 適用於檔案寫入作業 • `rename` 用於檔案重新命名作業 • `rename_dir` 用於目錄重新命名作業 • `setattr` 用於 Set 屬性作業 • `symlink` 用於符號連結作業 如果您指定 `-file-operations`、然後您必須在中指定有效的傳輸協定 `-protocol` 參數。	`-file-operations file_operations`、...

篩選 指定指定傳輸協定之特定檔案作業的篩選器清單。中的值 `-filters` 參數用於篩選用戶端要求。清單可包含下列一項或多項內容： ⓘ 如果您指定 `-filters` 參數、您也必須為指定有效值 `-file-operations` 和 `-protocol` 參數。 • `monitor-ads` 用於篩選用戶端要求的替代資料串流選項。 • `close-with-modification` 篩選用戶端要求以進行修改以關閉的選項。 • `close-without-modification` 篩選用戶端要求以關閉而不修改的選項。 • `first-read` 篩選用戶端要求以進行第一讀取的選項。 • `first-write` 篩選用戶端要求進行第一次寫入的選項。 • `offline-bit` 用於篩選用戶端離線位元集要求的選項。 設定此篩選器後、FPolicy伺服器只會在存取離線檔案時收到通知。 • `open-with-delete-intent` 用於篩選用戶端要求以進行「刪除目的」開啟的選項。 設定此篩選器後、FPolicy伺服器只會在嘗試開啟檔案以刪除檔案時收到通知。檔案系統會在使用時使用此功能 `FILE_DELETE_ON_CLOSE` 已指定旗標。 • `open-with-write-intent` 篩選用戶端要求以進行寫入目的開啟的選項。 設定此篩選器後、FPolicy伺服器只會在嘗試開啟檔案時收到通知、以便在其中寫入內容。 • `write-with-size-change` 選項可篩選用戶端寫入要求、並變更大小。	`-filters filter`、...

_Filters"（續） • `setattr-with-owner-change` 用於篩選用戶端設定檔要求以變更檔案或目錄擁有者的選項。 • `setattr-with-group-change` 用於篩選用戶端集點要求以變更檔案或目錄群組的選項。 • `setattr-with-sacl-change` 用於篩選用戶端集點要求以變更檔案或目錄上的 SACL 的選項。 此篩選器僅適用於SMB和NFSv4傳輸協定。 • `setattr-with-dacl-change` 用於篩選用戶端集點要求以變更檔案或目錄上的 DACL 的選項。 此篩選器僅適用於SMB和NFSv4傳輸協定。 • `setattr-with-modify-time-change` 用於篩選用戶端 setattr 要求以變更檔案或目錄的修改時間的選項。 • `setattr-with-access-time-change` 用於篩選用戶端 setattr 要求以變更檔案或目錄的存取時間的選項。 • `setattr-with-creation-time-change` 用於篩選用戶端 setattr 要求以變更檔案或目錄的建立時間的選項。 此選項僅適用於SMB傳輸協定。 • `setattr-with-mode-change` 用於篩選用戶端 setattr 要求以變更檔案或目錄上的模式位元的選項。 • `setattr-with-size-change` 用於篩選用戶端 setattr 要求以變更檔案大小的選項。 • `setattr-with-allocation-size-change` 用於篩選用戶端集點要求以變更檔案分配大小的選項。 此選項僅適用於SMB傳輸協定。 • `exclude-directory` 用於篩選用戶端目錄作業要求的選項。 指定此篩選器時、不會監控目錄作業。	`-filters filter`、 …
需要磁碟區作業 指定磁碟區掛載和卸載作業是否需要監控。預設值為 `false`。	`-volume-operation {true`

false} -filters filter、 ...	_FPolicy 存取遭拒通知 _ 從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。這些通知對於安全性、勒索軟體保護和治理來說非常重要。由於缺乏權限、將會產生檔案作業失敗的通知、其中包括： • NTFS 權限導致的失敗。 • 因 Unix 模式位元而發生故障。 • NFSv4 ACL 導致故障。
-monitor-fileop-failure {true	false}

FPolicy 可監控 **SMB** 的支援檔案作業和篩選器組合

設定FPolicy事件時、您必須注意、監控SMB檔案存取作業時、僅支援特定的檔案作業和篩選器組合。

下表提供了用於監控SMB檔案存取事件的FPolicy支援檔案操作和篩選器組合清單：

支援的檔案作業	支援的篩選器
關閉	監控廣告、離線位元、近距離修改、近距離不需修改、近距離讀取、 exclude目錄
建立	監控廣告、離線位元
create_dir	目前此檔案作業不支援篩選器。
刪除	監控廣告、離線位元
刪除目錄	目前此檔案作業不支援篩選器。
GetAttr	離線位元、exclude目錄
開啟	監控廣告、離線位元、開放刪除意圖、開放寫入目的、排除目錄
讀取	監控廣告、離線位元、第一讀取
寫入	監控廣告、離線位元、第一寫入、大小變更寫入

重新命名	監控廣告、離線位元
重新命名目錄	目前此檔案作業不支援篩選器。
設定	監控廣告、離線位元、設定ATtr_with _Owner_change、設定ATr_with _group_change、設定ATtr_with _mode_change、 setattr_with _SACL_change、setattr_with _dacl_change、setattr_with _dmodify_time_change、setattr_with _access_time_change、setattr_with creation_time_change、 setattr_with _size_change、setattr_with _all撥款_size_change、exclude目錄

從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。下表提供支援的存取遭拒檔案作業清單、以及 FPolicy 監控 SMB 檔案存取事件的篩選器組合：

支援的存取遭拒檔案作業	支援的篩選器
開啟	不適用

FPolicy 可監控 **NFSv3** 的支援檔案作業和篩選器組合

當您設定 FPolicy 事件時、您必須注意、只有特定的檔案作業和篩選器組合才支援監控 NFSv3 檔案存取作業。

下表提供支援的檔案作業清單、以及 FPolicy 監控 NFSv3 檔案存取事件的篩選組合：

支援的檔案作業	支援的篩選器
建立	離線位元
create_dir	目前此檔案作業不支援篩選器。
刪除	離線位元
刪除目錄	目前此檔案作業不支援篩選器。
連結	離線位元
查詢	離線位元、exclude目錄
讀取	離線位元、第一讀取
寫入	離線位元、第一寫入、大小變更寫入
重新命名	離線位元

重新命名目錄	目前此檔案作業不支援篩選器。
設定	離線位元、設定attr_with _Owner_change、設定attr_with _group變更、設定attr_with模式變更、設定ATtr_with修改時間變更、 setattr_with存取時間變更、setattr_with _size_change、exclude目錄
symlink	離線位元

從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。下表提供支援的拒絕存取檔案作業清單、以及 FPolicy 監控 NFSv3 檔案存取事件的篩選組合：

支援的存取遭拒檔案作業	支援的篩選器
存取	不適用
建立	不適用
create_dir	不適用
刪除	不適用
刪除目錄	不適用
連結	不適用
讀取	不適用
重新命名	不適用
重新命名目錄	不適用
設定	不適用
寫入	不適用

FPolicy可監控**NFSv4**的支援檔案操作和篩選器組合

設定FPolicy事件時、您必須注意、監控NFSv4檔案存取作業時、僅支援特定的檔案作業和篩選器組合。

下表提供NFSv4檔案存取事件FPolicy監控所支援的檔案操作和篩選器組合清單：

支援的檔案作業	支援的篩選器

關閉	離線位元、排除目錄
建立	離線位元
create_dir	目前此檔案作業不支援篩選器。
刪除	離線位元
刪除目錄	目前此檔案作業不支援篩選器。
GetAttr	離線位元、排除目錄
連結	離線位元
查詢	離線位元、排除目錄
開啟	離線位元、排除目錄
讀取	離線位元、第一讀取
寫入	離線位元、第一寫入、大小變更寫入
重新命名	離線位元
重新命名目錄	目前此檔案作業不支援篩選器。
設定	離線位元、設定attr_with _Owner_change、設定attr_with _group變更、設定ATr_with模式變更、設定ATtr_with _SACL_change、 setattr_with _dacl_change、setattr_with _dmodify_time_change、setattr_with _access_time_change、setattr_with _size_change、exclude目錄
symlink	離線位元

從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。下表提供支援的拒絕存取檔案作業清單、以及 FPolicy 監控 NFSv4 檔案存取事件的篩選組合：

支援的存取遭拒檔案作業	支援的篩選器
存取	不適用
建立	不適用
create_dir	不適用

刪除	不適用
刪除目錄	不適用
連結	不適用
開啟	不適用
讀取	不適用
重新命名	不適用
重新命名目錄	不適用
設定	不適用
寫入	不適用

完成**FPolicy**事件組態工作表

您可以使用這份工作表單來記錄FPolicy事件組態程序期間所需的值。如果需要參數值、您必須先判斷這些參數的值、再設定FPolicy事件。

您應該記錄是否要在FPolicy事件組態中包含每個參數設定、然後記錄您要納入的參數值。

資訊類型	必要	包括	您的價值
儲存虛擬機器（SVM）名稱	是的	是的	
事件名稱	是的	是的	
傳輸協定	否		
檔案作業	否		
篩選器	否		
Volume作業	否		
存取遭拒事件 （從 ONTAP 9.13 開始支援）	否		

規劃FPolicy原則組態

規劃FPolicy原則組態總覽

在設定FPolicy原則之前、您必須先瞭解建立原則時需要哪些參數、以及設定某些選用參數的原因。此資訊可協助您判斷要為每個參數設定哪些值。

建立FPolicy原則時、您會將原則與下列項目建立關聯：

- 儲存虛擬機器（SVM）
- 一或多個FPolicy事件
- FPolicy外部引擎

您也可以設定多個選用的原則設定。

FPolicy原則組態包含的內容

您可以使用下列可用的必要FPolicy原則清單和選用參數來協助規劃組態：

資訊類型	選項	必要	預設
*SVM*名稱 指定您要在其中建立FPolicy原則的SVM名稱。	`-vserver vserver_name`	是的	無
原則名稱 指定FPolicy原則的名稱。 名稱最長可達256個字元。 ⓘ 如果在MetroCluster 還原或SVM災難恢復組態中設定原則、名稱最長應為200個字元。 名稱可以包含下列任何Ascii範圍字元的組合： • `a` 透過 `z` • `A` 透過 `Z` • `0` 透過 `9` • “_” 、 “-”, and “.”	`-policy-name policy_name`	是的	無

事件名稱_ 指定要與FPolicy原則相關聯的以逗號分隔的事件清單。 • 您可以將多個事件與原則建立關聯。 • 事件是特定於傳輸協定的事件。 • 您可以使用單一原則來監控多個傳輸協定的檔案存取事件、方法是針對您要原則監控的每個傳輸協定建立事件、然後將事件與原則建立關聯。 • 事件必須已經存在。	`-events event_name`、...	是的	無
外部引擎名稱_ 指定要與FPolicy原則關聯的外部引擎名稱。 • 外部引擎包含節點傳送通知至FPolicy伺服器所需的資訊。 • 您可以將FPolicy設定為使用ONTAP 靜態原生外部引擎來進行簡單的檔案封鎖、或是使用外部引擎來設定使用外部FPolicy伺服器（FPolicy伺服器）來進行更精密的檔案封鎖和檔案管理。 • 如果您想要使用原生外部引擎、則無法指定此參數的值、也可以指定 `native` 做為價值。 • 如果您要使用FPolicy伺服器、則外部引擎的組態必須已經存在。	`-engine engine_name`	是（除非原則使用內部ONTAP 的非原生引擎）	`native`
是必填篩選 指定是否需要強制檔案存取篩選。 • 強制篩選設定可決定當所有主要和次要伺服器都當機、或在指定的逾時期間內未收到FPolicy伺服器的回應時、檔案存取事件會採取什麼行動。 • 設定為時 `true`、檔案存取事件遭拒。 • 設定為時 `false`，允許檔案存取事件。	`-is-mandatory {true`	`false}`	否

true	允許權限存取_ 指定您是否要FPolicy伺服器使用權限資料連線、以具有存取受監控檔案和資料夾的權限。 如果設定、FPolicy伺服器可以使用權限資料連線、從SVM的根目錄存取包含受監控資料的檔案。 若要進行特殊權限的資料存取、必須在叢集上授權 SMB 、且必須將用於連線至 FPolicy 伺服器的所有資料生命體設定為具有 `cifs` 作為其中一種允許的通訊協定。 如果您想要設定原則以允許權限存取、也必須為您想要FPolicy伺服器用於權限存取的帳戶指定使用者名稱。	`-allow -privileged -access` {yes	no}
否（除非啟用Passthrough-read）	`no`	特殊權限使用者名稱 指定FPolicy伺服器用來存取特殊權限資料的帳戶使用者名稱。 • 此參數的值應使用「'domain\username'」格式。 • 如果 `-allow -privileged -access` 設為 `no`，將忽略爲此參數設置的任何值。	`-privileged -user-name` `user_name`

否（除非已啟用權限存取）	無	允許Passthrough-read_ 指定FPolicy伺服器是否能為FPolicy伺服器歸檔至次要儲存設備（離線檔案）的檔案提供Passter-Read服務： • Passthsther-read是一種讀取離線檔案資料的方法、無需將資料還原至主要儲存設備。 Passthroh-read可減少回應延遲、因為在回應讀取要求之前、不需要將檔案重新叫用回主要儲存設備。此外、Passthrough-read可免除使用僅為了滿足讀取要求而回收的檔案來耗用主要儲存空間的需求、藉此優化儲存效率。 • 啟用時、FPolicy伺服器會透過專為Passthrough-Reads所開啟的個別特殊權限資料通道、提供檔案的資料。 • 如果您想要設定Passthrough-read、也必須將原則設定為允許權限存取。	`-is-passthrough-read-enabled {true`

如果**FPolicy**原則使用原生引擎、則需要**FPolicy**範圍組態

如果您將FPolicy原則設定為使用原生引擎、則需要針對原則設定的FPolicy範圍進行定義。

FPolicy範圍會定義套用FPolicy原則的界限、例如FPolicy是否套用至指定的磁碟區或共用區。有許多參數會進一步限制FPolicy原則套用的範圍。其中一個參數、 `-is-file-extension-check-on-directories`

`-enabled`，指定是否檢查目錄上的副檔名。預設值為 `false`，這表示不會檢查目錄上的副檔名。

當使用原生引擎的 FPolicy 原則在共用區或磁碟區和上啟用時 `-is-file-extension-check-on -directories-enabled` 參數設定為 `false` 對於原則的範圍、目錄存取會被拒絕。使用此組態時、因為不會檢查目錄的副檔名、所以如果目錄作業屬於原則範圍、則會拒絕任何目錄作業。

若要確保使用原生引擎時目錄存取成功、您必須設定 `-is-file-extension-check-on-directories -enabled parameter` 至 `true` 建立範圍時。

將此參數設為 `true`、會針對目錄作業進行延伸檢查、並根據 FPolicy 範圍組態中所包含或排除的延伸來決定是否允許或拒絕存取。

完成**FPolicy**原則工作表

您可以使用這份工作表單來記錄FPolicy原則組態程序期間所需的值。您應該記錄是否要在FPolicy原則組態中包含每個參數設定、然後記錄您要納入的參數值。

資訊類型	包括	您的價值
儲存虛擬機器（SVM）名稱	是的	
原則名稱	是的	
事件名稱	是的	
外部引擎名稱		
是否需要強制篩選？		
允許特殊權限存取		
權限使用者名稱		
是否已啟用Passthrough-read？		

規劃**FPolicy**範圍組態

規劃**FPolicy**範圍組態總覽

在設定FPolicy範圍之前、您必須先瞭解建立範圍的意義。您必須瞭解範圍組態包含哪些內容。您也需要瞭解優先順序的範圍規則。此資訊可協助您規劃要設定的值。

建立**FPolicy**範圍的意義

建立FPolicy範圍是指定義套用FPolicy原則的界限。儲存虛擬機器（SVM）是基本邊界。當您建立FPolicy原則的範圍時、必須定義要套用該原則的FPolicy原則、而且必須指定要套用範圍的SVM。

有許多參數會進一步限制指定SVM內的範圍。您可以指定要納入範圍的內容、或指定要從範圍中排除的項目、來限制範圍。將範圍套用至已啟用的原則之後、原則事件檢查就會套用至此命令所定義的範圍。

系統會針對檔案存取事件產生通知、其中「include'」選項中有相符項目。不會針對檔案存取事件產生通知、其中「exclude」選項中有相符項目。

FPolicy範圍組態定義下列組態資訊：

- SVM名稱
- 原則名稱
- 要納入或排除的共享區
- 匯出原則、以納入或排除受監控的內容
- 要納入或排除的磁碟區
- 要納入或排除的檔案副檔名
- 是否對目錄物件進行檔案副檔名檢查

> 叢集FPolicy原則的範圍有特殊考量。叢集FPolicy原則是叢集管理員為管理SVM所建立的原則。如果叢集管理員也為該叢集FPolicy原則建立範圍、則SVM管理員無法為該相同原則建立範圍。但是、如果叢集管理員未建立叢集FPolicy原則的範圍、則任何SVM管理員都可以建立該叢集原則的範圍。如果SVM管理員為該叢集FPolicy原則建立範圍、叢集管理員便無法隨後為該相同的叢集原則建立叢集範圍。這是因為叢集管理員無法覆寫同一個叢集原則的範圍。

優先順序的範圍規則為何

下列優先規則適用於範圍組態：

- 當共享區包含在中時 `-shares-to-include` 共享區的參數和父Volume會包含在中 `-volumes-to-exclude` 參數、 `-volumes-to-exclude` 優先於 `-shares-to-include`。
- 當中包含匯出原則時 `-export-policies-to-include` 匯出原則的參數和父Volume會包含在中 `-volumes-to-exclude` 參數、 `-volumes-to-exclude` 優先於 `-export-policies-to-include`。
- 系統管理員可以同時指定兩者 `-file-extensions-to-include` 和 `-file-extensions-to-exclude` 清單。

  。 `-file-extensions-to-exclude` 參數會在之前檢查 `-file-extensions-to-include` 參數已核取。

FPolicy範圍組態包含的內容

您可以使用下列可用的FPolicy範圍組態參數清單來協助規劃組態：

> 當設定要納入或排除範圍的共用、匯出原則、磁碟區及副檔名時、包含和排除參數可以包含像是「」之類的元元符號?" and "*。 不支援使用規則運算式。

資訊類型	選項

SVM 指定您要在其中建立FPolicy範圍的SVM名稱。 每個FPolicy組態都是在單一SVM中定義。為了建立FPolicy原則組態、而將外部引擎、原則事件、原則範圍和原則結合在一起的原則、都必須與相同的SVM建立關聯。	`-vserver vserver_name`
原則名稱 指定要附加範圍的FPolicy原則名稱。FPolicy原則必須已經存在。	`-policy-name policy_name`
要納入的共享_ 指定以逗號分隔的共用清單、以監控套用範圍的FPolicy原則。	`-shares-to-include share_name、 ...`
要排除的共享_ 指定要從套用範圍之FPolicy原則的監控中排除的以逗號分隔的共用清單。	`-shares-to-exclude share_name、 ...`
_要包含的磁碟區_指定以逗號分隔的磁碟區清單、以監控套用範圍的FPolicy原則。	`-volumes-to-include volume_name、 ...`
要排除的磁碟區_ 指定要從套用範圍之FPolicy原則的監控中排除的以逗號分隔的磁碟區清單。	`-volumes-to-exclude volume_name、 ...`
匯出要納入的原則_ 指定以逗號分隔的匯出原則清單、以監控套用範圍的FPolicy原則。	`-export-policies-to -include export_policy_name、 ...`
匯出要排除的原則_ 指定要從套用範圍之FPolicy原則的監控中排除的匯出原則清單（以英文分隔）。	`-export-policies-to -exclude export_policy_name、 ...`
要包括的副檔名 指定要監控套用範圍之FPolicy原則的檔案副檔名以逗號分隔的清單。	`-file-extensions-to -include file_extensions、 ...`
要排除的檔案副檔名_ 指定要從套用範圍之FPolicy原則的監控中排除的檔案副檔名以逗號分隔的清單。	`-file-extensions-to -exclude file_extensions、 ...`

檔案副檔名檢查是否已啟用目錄？ 指定副檔名檢查是否也適用於目錄物件。如果此參數設為 `true`，目錄物件會受到與一般檔案相同的副檔名檢查。如果此參數設為 `false`，目錄名稱不符合副檔名，即使目錄的副檔名不符，也會傳送通知給目錄。 如果將範圍指派給的 FPolicy 原則設定為使用原生引擎、則必須將此參數設定為 `true`。	`-is-file-extension -check-on-directories -enabled {true`
`false`	}

完成**FPolicy**範圍工作表

您可以使用這份工作表單來記錄FPolicy範圍組態程序期間所需的值。如果需要參數值、您必須先判斷這些參數的使用值、然後再設定FPolicy範圍。

您應該記錄是否要在FPolicy範圍組態中包含每個參數設定、然後記錄您要納入的參數值。

資訊類型	必要	包括	您的價值
儲存虛擬機器（SVM）名稱	是的	是的	
原則名稱	是的	是的	
要納入的共享區	否		
要排除的共享區	否		
要包含的磁碟區	否		
要排除的磁碟區	否		
匯出要納入的原則	否		
匯出要排除的原則	否		
要包含的副檔名	否		
要排除的副檔名	否		
是否已啟用目錄的副檔名檢查？	否		

建立**FPolicy**組態

建立FPolicy外部引擎

您必須建立外部引擎、才能開始建立FPolicy組態。外部引擎定義FPolicy如何建立及管理外部FPolicy伺服器的連線。如果您的組態使用內部ONTAP 的靜態引擎（原生外部引擎）來進行簡單的檔案封鎖、則不需要設定個別的FPolicy外部引擎、也不需要執行此步驟。

您需要的產品

- "外部引擎" 工作表應填寫完畢。

關於這項工作

如果外部引擎用於MetroCluster 整個功能表組態、您應該將來源站台的FPolicy伺服器IP位址指定為主要伺服器。目的地站台FPolicy伺服器的IP位址應指定為次要伺服器。

步驟

1. 使用建立 FPolicy 外部引擎 `vserver fpolicy policy external-engine create` 命令。

   下列命令會在儲存虛擬機器（SVM）vs1.example.com上建立外部引擎。與FPolicy伺服器的外部通訊不需要驗證。

   ```
   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. 使用驗證 FPolicy 外部引擎組態 `vserver fpolicy policy external-engine show` 命令。

   下列命令會顯示有關SVM vs1.example.com上設定的所有外部引擎資訊：

   ```
   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
   ```

   下列命令會在SVM vs1.example.com上顯示名為「engin1」的外部引擎詳細資訊：

   ```
   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: -
```

建立FPolicy事件

在建立FPolicy原則組態時、您需要建立FPolicy事件。您可以在建立事件時、將其與FPolicy原則建立關聯。事件會定義要監控的傳輸協定、以及要監控和篩選的檔案存取事件。

開始之前

您應該完成 FPolicy 活動 "工作表"。

建立**FPolicy**事件

1. 使用建立 FPolicy 事件 `vserver fpolicy policy event create` 命令。

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

2. 使用驗證 FPolicy 事件組態 `vserver fpolicy policy event show` 命令。

   ```
   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
   ```

建立 **FPolicy** 存取遭拒事件

從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。這些通知對於安全性、勒索軟體保護和治理來說非常重要。

1. 使用建立 FPolicy 事件 `vserver fpolicy policy event create` 命令。

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

建立持續儲存區

從 ONTAP 9.14.1 開始、 FPolicy 可讓您設定 "持續儲存區" 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。

最佳實務做法

- 在使用持續儲存功能之前、請確保您的合作夥伴應用程式支援此組態。
- 持續儲存區 Volume 是以每個 SVM 為基礎進行設定。對於每個啟用 FPolicy 的 SVM 、您都需要一個持續儲存區 Volume 。
- 建立磁碟區時指定的持續儲存區磁碟區名稱和交會路徑應相符。
- 在具有預期由 Fpolicy 監控最大流量的生命期的節點上建立持續儲存區磁碟區。
- 將 Snapshot 原則設為 `none` 而非 `default`。這是為了確保不會意外還原快照而導致目前事件遺失、並防止可能的重複事件處理。
- 讓外部使用者傳輸協定存取（ CIFS/NFS ）無法存取持續儲存區磁碟區、以避免意外毀損或刪除持續存在的事件記錄。為達成此目的、在啟用 FPolicy 之後、請在 ONTAP 中卸載磁碟區以移除連接路徑、這會使使用者傳輸協定存取無法存取。

步驟

1. 在 SVM 上建立一個空的磁碟區、以便為持續儲存區進行資源配置：

   ```
   volume create -vserver <SVM Name> -volume <volume> -state <online> -junction
   -path <path> -policy <default> -unix-permissions <777> -size <value>
   -aggregate <aggregate name> -snapshot-policy <none>
   ```

   - 持續儲存區磁碟區的大小取決於您要持續處理未傳送至外部伺服器（合作夥伴應用程式）的事件所需的時間。

     例如、如果您想要在每秒有 30K 通知的叢集中保留 30 分鐘的事件容量：

     所需 Volume 大小 = 30000 x 30 x 60 x 0.6KB （平均通知記錄大小） = 32400000 KB = ~32 GB

   若要找出大約的通知率、您可以聯絡 FPolicy 合作夥伴應用程式、或使用 FPolicy 計數器 `requests_dispatched_rate`。

   - 系統管理員使用者若擁有足夠的 RBAC 權限（以建立磁碟區）、則應使用 Volume CLI 命令或 REST API 建立所需大小的磁碟區、並提供該磁碟區的名稱做為 `-volume` 在持續儲存區中、建立 CLI 命令或 REST API 。
2. 建立持續儲存區：

   ```
   vserver fpolicy persistent store create -vserver <SVM> -persistent-store
   <PS_name> -volume <volume>
   ```

   - Persistent-store ：持續儲存區名稱

- Volume ：持續儲存區 Volume

3. 建立持續儲存區之後、您可以建立 FPolicy 原則、並將持續儲存區名稱新增至該原則。 如需詳細資訊、請參閱 "建立FPolicy原則"。

建立FPolicy原則

當您建立FPolicy原則時、會將外部引擎和一或多個事件與原則建立關聯。此原則也會指定是否需要強制篩選、FPolicy伺服器是否具有存取儲存虛擬機器（SVM）上資料的權限、以及是否啟用離線檔案的傳遞讀取。

您需要的產品

- FPolicy原則工作表應完成。
- 如果您打算設定原則使用FPolicy伺服器、則外部引擎必須存在。
- 您計畫與FPolicy原則建立關聯的FPolicy事件必須至少存在一個。
- 如果您要設定特殊權限資料存取、SVM上必須有SMB伺服器。
- 若要設定原則的持續儲存區、引擎類型必須為 * 非同步 * 、原則必須為 * 非強制 * 。

  如需詳細資訊、請參閱 "建立持續儲存區"。

步驟

1. 建立FPolicy原則：

   ```
   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}]
   ```

   - 您可以將一或多個事件新增至FPolicy原則。
   - 預設會啟用強制篩選。
   - 如果您想要透過設定來允許特殊權限存取 `-allow-privileged-access` 參數至 `yes`、您也必須設定權限使用者名稱以進行權限存取。
   - 如果您想要設定 Passthrough-read 、請設定 `-is-passthrough-read-enabled` 參數至 `true`、您也必須設定特殊權限資料存取。

     下列命令會建立名為「policy1'」的原則、其事件名稱為「EVENT1」、外部引擎名稱為「engine 1'」。此原則會在原則組態中使用預設值： `vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

     下列命令會建立名為「policy2」的原則、其事件名稱為「'Event2」、外部引擎名稱為「engine 2」。此原則設定為使用指定的使用者名稱來使用權限存取。Passthsthread-read已啟用：

     ```
     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
     ```

下列命令會建立名為「native1」的原則、並將事件命名為「事件3」。此原則使用原生引擎、並在原則組態中使用預設值：

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

2. 使用驗證 FPolicy 原則組態 `vserver fpolicy policy show` 命令。

   下列命令會顯示有關三個已設定的FPolicy原則的資訊、包括下列資訊：

   - 與原則相關聯的SVM
   - 與原則相關聯的外部引擎
   - 與原則相關的事件
   - 是否需要強制篩選
   - 是否需要權限存取 `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
```

建立FPolicy範圍

建立FPolicy原則之後、您需要建立FPolicy範圍。建立範圍時、您會將範圍與FPolicy原則建立關聯。範圍會定義套用FPolicy原則的界限。範圍可以根據共用、匯出原則、磁碟區和副檔名來包含或排除檔案。

您需要的產品

必須填寫FPolicy範圍工作表。FPolicy原則必須與關聯的外部引擎一起存在（如果原則設定為使用外部FPolicy伺服器）、且必須至少有一個關聯的FPolicy事件。

步驟

1. 使用建立 FPolicy 範圍 `vserver fpolicy policy scope create` 命令。

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

2. 使用驗證 FPolicy 範圍組態 `vserver fpolicy policy scope show` 命令。

```
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: -
```

啟用**FPolicy**原則

完成FPolicy原則組態設定之後、您就可以啟用FPolicy原則。啟用原則會設定其優先順序、並開始監控原則的檔案存取。

您需要的產品

FPolicy原則必須與關聯的外部引擎一起存在（如果原則設定為使用外部FPolicy伺服器）、且必須至少有一個關聯的FPolicy事件。FPolicy原則範圍必須存在、而且必須指派給FPolicy原則。

關於這項工作

當在儲存虛擬機器（SVM）上啟用多個原則、且有多個原則已訂閱相同的檔案存取事件時、就會使用優先順序。使用原生引擎組態的原則優先順序高於任何其他引擎的原則、無論啟用原則時指派給它們的順序編號為何。

> 無法在管理SVM上啟用原則。

步驟

1. 使用啟用 FPolicy 原則 `vserver fpolicy enable` 命令。

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

2. 使用確認 FPolicy 原則已啟用 `vserver fpolicy show` 命令。

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

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

管理 FPolicy 組態

修改FPolicy組態

修改FPolicy組態的命令

您可以修改組成組態的元素、以修改FPolicy組態。您可以修改外部引擎、FPolicy事件、FPolicy範圍及FPolicy原則。您也可以啟用或停用FPolicy原則。當您停用FPolicy原則時、該原則的檔案監控將會中斷。

建議在修改組態之前先停用FPolicy原則。

如果您要修改…	使用此命令…
外部引擎	`vserver fpolicy policy external-engine modify`
活動	`vserver fpolicy policy event modify`
範圍	`vserver fpolicy policy scope modify`
原則	`vserver fpolicy policy modify`

如需詳細資訊、請參閱命令的手冊頁。

啟用或停用FPolicy原則

您可以在組態完成後啟用FPolicy原則。啟用原則會設定其優先順序、並開始監控原則的檔案存取。若要停止原則的檔案存取監控、您可以停用FPolicy原則。

您需要的產品

在啟用FPolicy原則之前、必須先完成FPolicy組態。

關於這項工作

- 當在儲存虛擬機器（SVM）上啟用多個原則、且有多個原則已訂閱相同的檔案存取事件時、就會使用優先順序。
- 使用原生引擎組態的原則優先順序高於任何其他引擎的原則、無論啟用原則時指派給它們的順序編號為何。
- 若要變更FPolicy原則的優先順序、您必須停用該原則、然後使用新的順序編號重新啟用。

步驟

1. 執行適當的行動：

如果您想要…	輸入下列命令…
啟用FPolicy原則	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`

停用FPolicy原則	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

顯示**FPolicy**組態的相關資訊

show命令的運作方式

在顯示有關 FPolicy 組態的資訊以瞭解的方式時、這很有幫助 `show` 命令運作正常。

答 `show` 不含其他參數的命令會以摘要形式顯示資訊。此外、每個 `show` Command 具有相同的兩個互斥選擇性參數、 `-instance` 和 `-fields`。

當您使用時 `-instance` 參數與 `show` 命令時、命令輸出會以清單格式顯示詳細資訊。在某些情況下、詳細輸出可能會很長、而且包含的資訊比您需要的還多。您可以使用 `-fields fieldname[,fieldname…]` 此參數可自訂輸出、使其僅顯示指定欄位的資訊。您可以輸入來識別您可以指定的欄位 `?` 之後 `-fields` 參數。

> 的輸出 `show` 命令 `-fields` 參數可能會顯示與所要求欄位相關的其他相關和必要欄位。

每個 `show` 命令具有一個或多個可選參數，用於篩選輸出結果，並使您能夠縮小命令輸出中顯示的信息範圍。您可以輸入、識別命令可使用的選用參數 `?` 之後 `show` 命令。

。 `show` 命令支援 UNIX 樣式的模式和萬用字元、可讓您在命令參數引數中比對多個值。例如、您可以使用萬用字元運算子（*）、非運算子（！）、OR運算子（|）、範圍運算子（integer…integer）、小於運算子（<）、大於運算子（>）、小於或等於運算子（<=）、以及大於或等於運算子（>=）來指定值。

如需使用UNIX樣式模式和萬用字元的詳細資訊、請參閱 使用ONTAP 指令行介面。

用於顯示**FPolicy**組態資訊的命令

您可以使用 `fpolicy show` 顯示 FPolicy 組態相關資訊的命令、包括有關 FPolicy 外部引擎、事件、範圍和原則的資訊。

如果您要顯示FPolicy的相關資訊…	使用此命令…
外部引擎	`vserver fpolicy policy external-engine show`
活動	`vserver fpolicy policy event show`
範圍	`vserver fpolicy policy scope show`
原則	`vserver fpolicy policy show`

如需詳細資訊、請參閱命令的手冊頁。

顯示**FPolicy**原則狀態的相關資訊

您可以顯示FPolicy原則狀態的相關資訊、以判斷原則是否已啟用、原則要使用的外部引擎、原則的順序編號、以及FPolicy原則與哪個儲存虛擬機器（SVM）相關聯。

關於這項工作

如果未指定任何參數、命令會顯示下列資訊：

- SVM名稱
- 原則名稱
- 原則順序編號
- 原則狀態

除了顯示叢集或特定SVM上所設定之FPolicy原則的原則狀態資訊、您也可以使用命令參數、依其他條件篩選命令的輸出。

您可以指定 `-instance` 顯示所列原則詳細資訊的參數。或者、您也可以使用 `-fields` 參數、僅顯示命令輸出或中指定的欄位 `-fields ?` 決定您可以使用哪些欄位。

步驟

1. 使用適當的命令顯示FPolicy原則狀態的篩選資訊：

如果您要顯示原則的狀態資訊…	輸入命令…
在叢集上	`vserver fpolicy show`
具有指定狀態的	`vserver fpolicy show -status {on
off}`	在指定的SVM上
`vserver fpolicy show -vserver vserver_name`	使用指定的原則名稱
`vserver fpolicy show -policy-name policy_name`	使用指定的外部引擎

範例

下列範例顯示叢集上FPolicy原則的相關資訊：

```
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
```

顯示已啟用**FPolicy**原則的相關資訊

您可以顯示已啟用FPolicy原則的相關資訊、以判斷其設定使用的FPolicy外部引擎、原則的優先順序、以及FPolicy原則關聯的儲存虛擬機器（SVM）。

關於這項工作

如果未指定任何參數、命令會顯示下列資訊：

- SVM名稱
- 原則名稱
- 原則優先順序

您可以使用命令參數、根據指定的條件篩選命令的輸出。

步驟

1. 使用適當的命令顯示已啟用的FPolicy原則相關資訊：

如果您要顯示已啟用原則的相關資訊…	輸入命令…
在叢集上	`vserver fpolicy show-enabled`
在指定的SVM上	`vserver fpolicy show-enabled -vserver vserver_name`
使用指定的原則名稱	`vserver fpolicy show-enabled -policy-name policy_name`
使用指定的序號	`vserver fpolicy show-enabled -priority integer`

範例

下列範例顯示叢集上已啟用FPolicy原則的相關資訊：

```
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
```

管理**FPolicy**伺服器連線

連線至外部**FPolicy**伺服器

若要啟用檔案處理、您可能需要手動連線至外部FPolicy伺服器（如果先前已終止連線）。連線會在伺服器逾時後終止、或因為發生錯誤而終止。或者、系統管理員也可以手動終止連線。

關於這項工作

如果發生嚴重錯誤、則可終止與FPolicy伺服器的連線。解決造成嚴重錯誤的問題之後、您必須手動重新連線至FPolicy伺服器。

步驟

1. 使用連線至外部 FPolicy 伺服器 `vserver fpolicy engine-connect` 命令。

   如需命令的詳細資訊、請參閱手冊頁。

2. 使用確認外部 FPolicy 伺服器已連線 `vserver fpolicy show-engine` 命令。

   如需命令的詳細資訊、請參閱手冊頁。

中斷與外部**FPolicy**伺服器的連線

您可能需要手動中斷與外部FPolicy伺服器的連線。如果FPolicy伺服器在處理通知要求時發生問題、或是您需要在FPolicy伺服器上執行維護、則可能需要這樣做。

步驟

1. 使用中斷與外部 FPolicy 伺服器的連線 `vserver fpolicy engine-disconnect` 命令。

   如需命令的詳細資訊、請參閱手冊頁。

2. 使用確認外部 FPolicy 伺服器已中斷連線 `vserver fpolicy show-engine` 命令。

   如需命令的詳細資訊、請參閱手冊頁。

顯示與外部**FPolicy**伺服器連線的相關資訊

您可以顯示叢集或特定儲存虛擬機器（SVM）與外部FPolicy伺服器（FPolicy伺服器）連線的狀態資訊。此資訊可協助您判斷哪些FPolicy伺服器已連線。

關於這項工作

如果未指定任何參數、命令會顯示下列資訊：

- SVM名稱
- 節點名稱
- FPolicy原則名稱
- FPolicy伺服器IP位址
- FPolicy伺服器狀態
- FPolicy伺服器類型

除了顯示叢集或特定SVM上FPolicy連線的相關資訊、您也可以使用命令參數、根據其他條件篩選命令的輸出。

您可以指定 `-instance` 顯示所列原則詳細資訊的參數。或者、您也可以使用 `-fields` 此參數僅顯示命令輸出中指定的欄位。您可以輸入 `?` 之後 `-fields` 參數來找出您可以使用的欄位。

步驟

1. 使用適當的命令、顯示節點與FPolicy伺服器之間連線狀態的篩選資訊：

如果您要顯示FPolicy伺服器的連線狀態資訊…	輸入…
您指定的	`vserver fpolicy show-engine -server IP_address`
適用於指定的SVM	`vserver fpolicy show-engine -vserver vserver_name`
隨附於指定原則的	`vserver fpolicy show-engine -policy-name policy_name`
使用您指定的伺服器狀態	`vserver fpolicy show-engine -server-status status` 伺服器狀態可以是下列其中一項： • `connected` • `disconnected` • `connecting` • `disconnecting`

使用指定類型	`vserver fpolicy show-engine -server-type type` FPolicy伺服器類型可以是下列其中一種： • `primary` • `secondary`
已中斷連線的原因	`vserver fpolicy show-engine -disconnect-reason text` 中斷連線可能有多種原因。以下是中斷連線的常見原因： • `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.`

範例

此範例顯示SVM vs1.example.com上的FPolicy伺服器外部引擎連線相關資訊：

```
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
```

此範例僅顯示連線的FPolicy伺服器相關資訊：

```
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
```

顯示有關**FPolicy Passthrough-read**連線狀態的資訊

您可以針對叢集或特定儲存虛擬機器（SVM）、顯示與外部FPolicy伺服器（FPolicy伺服器）的FPolicy Passthrough-read連線狀態相關資訊。此資訊可協助您判斷哪些FPolicy伺服器具有直通讀取資料連線、以及哪些FPolicy伺服器的直通讀取連線中斷。

關於這項工作

如果未指定任何參數、命令會顯示下列資訊：

- SVM名稱
- FPolicy原則名稱
- 節點名稱
- FPolicy伺服器IP位址
- FPolicy Passthrough-read連線狀態

除了顯示叢集或特定SVM上FPolicy連線的相關資訊、您也可以使用命令參數、根據其他條件篩選命令的輸出。

您可以指定 `-instance` 顯示所列原則詳細資訊的參數。或者、您也可以使用 `-fields` 此參數僅顯示命令輸出中指定的欄位。您可以輸入 `?` 之後 `-fields` 參數來找出您可以使用的欄位。

步驟

1. 使用適當的命令、顯示節點與FPolicy伺服器之間連線狀態的篩選資訊：

如果您要顯示有關…的連線狀態資訊	輸入命令…
叢集的FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection`
指定SVM的FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`
指定原則的FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
指定原則的詳細FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`

您指定狀態的FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status` 伺服器狀態可以是下列其中一項： • `connected` • `disconnected`

範例

下列命令會顯示叢集上所有FPolicy伺服器的Passthrough-read連線相關資訊：

```
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
```

下列命令會顯示「'pol_CIFS _1'」原則中所設定之FPolicy伺服器的Passthrough-read連線詳細資訊：

```
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
```

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。