規劃FPolicy組態

ONTAP 9

NetApp
February 12, 2026

目錄

規劃FPolicy組態

配置 ONTAP FPolicy 的要求、注意事項和最佳實踐

在儲存虛擬機器（SVM）上建立及設定FPolicy組態之前、您必須瞭解設定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 ONTAP 9 8 開始、 ONTAP 提供用戶端 LIF 服務 `data-fpolicy-client`、用於外傳 FPolicy 連線、並新增服務。"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。

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。

持續儲存區

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。

- 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。
- 每個啟用 FPolicy 的 SVM 都需要一個持續儲存區。
  - 每個 SVM 只能設定一個持續儲存區。此單一持續儲存區必須用於該 SVM 上的所有 FPolicy 組態、即使這些原則來自不同的合作夥伴。
- ONTAP 9.15.1 或更新版本：
  - 當您建立持續儲存區時、會自動處理持續儲存區、其磁碟區及其磁碟區組態。
- ONTAP 9.14.1 ：
  - 持續儲存區、其磁碟區及其磁碟區組態是手動處理的。
- 在節點上建立持續儲存區磁碟區、其中包含預期由 FPolicy 監控的最大流量。
  - ONTAP 9.15.1 或更新版本：磁碟區會在持續儲存區建立期間自動建立及設定。
  - ONTAP 9.14.1 ：叢集管理員必須在啟用 FPolicy 的每個 SVM 上建立及設定持續儲存區的磁碟區。
- 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 就會開始以適當的 EMS 訊息來丟棄傳入通知。
  - ONTAP 9.15.1 或更新版本：除了 `size` 參數 `autosize-mode` 參數可協助磁碟區隨使用空間量而增加或縮小。
  - ONTAP 9.14.1 `size` 在磁碟區建立期間設定參數、以提供最大限制。
- 將 Snapshot 原則設為 `none` 用於永久儲存區 Volume 、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。
  - ONTAP 9.15.1 或更新版本 `snapshot-policy` 在持續儲存區建立期間、參數會自動設定為無。
  - ONTAP 9.14.1 `snapshot-policy` 參數設定為 `none` 在磁碟區建立期間。
- 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。
  - ONTAP 9.15.1 或更新版本： ONTAP 會在持續儲存區建立期間、自動封鎖磁碟區、使其無法存取外部使用者傳輸協定（ CIFS/NFS ）。
  - ONTAP 9.14.1 ：啟用 FPolicy 之後、請在 ONTAP 中卸載 Volume 以移除連接路徑。這使得外部使用者傳輸協定存取（ CIFS/NFS ）無法存取。

如需詳細資訊、請參閱 "FPolicy 永續性儲存區" 和 "建立持續儲存區"。

持續儲存區容錯移轉和恢復

持續儲存區會維持上次收到事件、發生非預期的重新開機、或是停用 FPolicy 並再次啟用時的狀態。在接管作業之後、新事件會由合作夥伴節點儲存和處理。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。

如果持久性儲存磁碟區從同一 SVM 中的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。您需要重新運行 `fpolicy persistent-store create`移動磁碟區後，在任一節點上執行指令，以確保待處理的通知傳遞到外部伺服器。

詳細了解 `fpolicy persistent-store create`在"指令參考資料ONTAP" 。

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

計數器	說明
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 counters *
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

深入瞭解 `statistics start`及 `statistics show` "指令參考資料ONTAP"。

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、請確定 FPolicy 原則中沒有任何一個具有設定的持續儲存區。如果設定持續儲存區、還原將會失敗。

相關資訊

- "統計數據顯示"
- "統計開始"

設定 ONTAP FPolicy 配置

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。

   從 ONTAP 9.15.1 開始、您可以使用 `protobuf` 引擎格式。設定為時 `protobuf`、通知訊息會使用Google Prototbuf以二進位格式編碼。將引擎格式設定為之前 `protobuf`，請確保 FPolicy 伺服器也支援 `protobuf` 反序列化。如需詳細資訊、請參閱 "規劃FPolicy外部引擎組態"

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 持續儲存區（選用）。

   從 ONTAP 9.14.1 開始、 FPolicy 可讓您進行設定 "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。不支援同步（強制或非強制）和非同步強制組態。

   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 9.15.1 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 、並設定持續儲存區的 Volume 。

4. 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。

5. 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。

6. 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 ONTAP FPolicy 外部引擎配置

設定 FPolicy 外部引擎之前、您必須先瞭解建立外部引擎的意義、以及哪些組態參數可供使用。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 需要建立及管理外部 FPolicy 伺服器連線的資訊、包括：

- 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
- 引擎格式是否為 `xml` 或 `protobuf`

  從 ONTAP 9.15.1 開始、您可以使用 `protobuf` 引擎格式。設定為時 `protobuf`、通知訊息會使用Google Prototbuf以二進位格式編碼。將引擎格式設定為之前 `protobuf`，請確保 FPolicy 伺服器也支援 `protobuf` 反序列化。

由於支援的 probuf 格式從 ONTAP 9.15.1 開始、因此您必須先考慮外部引擎格式、才能還原至舊版 ONTAP 。如果您恢復為 ONTAP 9.15.1 之前的版本、請與 FPolicy 合作夥伴合作、以：

- 從變更每個引擎格式 `protobuf` 至 `xml`
- 刪除引擎格式為的引擎 `protobuf`

- 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`
外部引擎格式_ 指定外部引擎格式是 XML 還是 protobuf 。 從 ONTAP 9.15.1 開始、您可以使用原型引擎格式。設為 probuf 時、通知訊息會使用 Google Prototbuf 以二進位格式編碼。在將引擎格式設定為 protobuf 之前、請確定 FPolicy 伺服器也支援 protobuf 反序列化。	`- extern-engine-format {protobuf 或 xml}`

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]`

有關配置 ONTAP FPolicy 外部引擎以使用 SSL 身份驗證連接的其他信息

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，請勿刪除此憑證。

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`。

相關資訊

- "安全性憑證安裝"

ONTAP FPolicy 憑證不會在具有非 ID 保留配置的 SVM 災難復原關係中複製

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 ）。

相關資訊

- "SnapMirror建立"

具有 **MetroCluster** 和 **SVM** 災難復原配置的叢集範圍 **ONTAP FPolicy** 外部引擎的限制

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 **ONTAP FPolicy** 外部引擎設定工作表

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

瞭解 ONTAP FPolicy 事件組態

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 可監控 SMB ， NFSv3 ， NFSv4 ，以及從 ONTAP 9.15.1 開始的 NFSv4.1 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。 從 ONTAP 9.15.1 開始， NFSv4 可讓您擷取 NFSv4.0 和 NFSv4.1 事件。	`-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。 • `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	`-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}`

ONTAP FPolicy 監控 SMB 支援的檔案操作和過濾器組合

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

ONTAP FPolicy 為 NFSv3 監控的支援的檔案操作和過濾器組合

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

ONTAP FPolicy 為 NFSv4 監控的支援的檔案操作和過濾器組合

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。

從 ONTAP 9.15.1 開始、 FPolicy 支援 NFSv4.1 傳輸協定。

下表提供 NFSv4 或 NFSv4.1 檔案存取事件的 FPolicy 監控支援檔案作業和篩選器組合清單：

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 或 NFSv4.1 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 **ONTAP FPolicy** 事件設定工作表

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

了解 ONTAP FPolicy 策略配置

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
Persistent story 從 ONTAP 9.14.1 開始、此參數會指定持續儲存區、以擷取 SVM 中非強制性非非同步原則的檔案存取事件。	`-persistent -store persistent_store_name`	否	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** 政策使用本機引擎，則需要 **ONTAP FPolicy** 範圍配置

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 **ONTAP FPolicy** 策略工作表

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	
持續儲存區		
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

了解 **ONTAP FPolicy** 範圍配置

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 **ONTAP 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		