建立FPolicy組態

ONTAP 9

NetApp
February 12, 2026

目錄

建立FPolicy組態

創建 ONTAP 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。

開始之前

。 "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 ONTAP 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 事件"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 ONTAP FPolicy 持久性存儲

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、 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。

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 。

根據 ONTAP 版本的不同、有兩種方法可以建立持續儲存區：

- ONTAP 9.15.1 或更新版本：當您建立持續儲存區時、 ONTAP 會自動同時建立及設定其 Volume 。如此可簡化 FPolicy 持續儲存區組態、並實作所有最佳實務做法。
- ONTAP 9.14.1 ：手動建立和設定磁碟區、然後為新建立的磁碟區建立持續儲存區。

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。

建立持續儲存區（ ONTAP 9.15.1 或更新版本）

從 ONTAP 9.15.1 開始、請使用 `fpolicy persistent-store create` 命令來建立具有內嵌磁碟區建立和組態的 FPolicy 持續儲存區。ONTAP 會自動封鎖磁碟區、使其無法存取外部使用者傳輸協定（ CIFS/NFS ）。

開始之前

- 您要建立持續儲存區的 SVM 必須至少有一個集合體。
- 您應該可以存取 SVM 可用的集合體、並擁有足夠的權限來建立 Volume 。

步驟

1. 建立持續儲存區、以自動建立和設定磁碟區：

```
vserver fpolicy persistent-store create -vserver <vserver> -persistent-store
<name> -volume <volume_name> -size <size> -autosize-mode
<off|grow|grow_shrink>
```

   - 。 `vserver` 參數是 SVM 的名稱。
   - 。 `persistent-store` 參數是持續儲存區的名稱。
   - 。 `volume` 參數是持續儲存區磁碟區的名稱。

     如果您想要使用現有的空白磁碟區、請使用 `volume show` 命令來尋找它、並在 Volume 參數中指定它。

   - 。 `size` 參數是根據您想要保留未傳送至外部伺服器（合作夥伴應用程式）的事件的持續時間。

     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

要查找大致的通知率，您可以聯繫您的 FPolicy 合作伙伴應用程序或使用 FPolicy 計數器 `requests_dispatched_rate`。

如果您使用現有的 Volume 、則 Size 參數為選用項目。如果您確實為 size 參數提供值、它會以您指定的大小修改 Volume 。

- 。 `autosize-mode` 參數指定 Volume 的自動調整模式。支援的自動調整大小模式包括：
  - Off （關） - 磁碟區不會因應使用空間量而增加或縮小大小。
  - 擴充 - 當磁碟區中的使用空間超過擴充臨界值時、磁碟區會自動增加。
  - GROW _ 收縮：磁碟區會隨著使用空間的數量而增加或縮小大小。

2. 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"。

建立持續儲存區（ **ONTAP 9.14.1** ）

您可以建立磁碟區、然後建立持續儲存區以使用該磁碟區。接著、您可以封鎖新建立的 Volume 、使其無法存取外部使用者傳輸協定（ CIFS/NFS ）。

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> -policy
<default> -unix-permissions <777> -size <value> -aggregate <aggregate name>
-snapshot-policy <none>
```

系統管理員使用者若擁有足夠的 RBAC 權限（以建立 Volume ）、就會建立所需大小的 Volume （使用 Volume CLI 命令或 REST API ）、並提供該 Volume 的名稱做為 `-volume` 在持續儲存區中、建立 CLI 命令或 REST API 。

- 。 `vserver` 參數是 SVM 的名稱。
- 。 `volume` 參數是持續儲存區磁碟區的名稱。
- 。 `state` 參數應設為線上、以便使用 Volume 。
- 。 `policy` 如果您已設定 FPolicy 服務原則、則參數會設為 FPolicy 服務原則。如果沒有、您可以使用 `volume modify` 命令稍後新增原則。
- 。 `unix-permissions` 參數為選用項目。
- 。 `size` 參數是根據您想要保留未傳送至外部伺服器（合作夥伴應用程式）的事件的持續時間。

  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

要查找大致的通知率，您可以聯繫您的 FPolicy 合作伙伴應用程序或使用 FPolicy 計數器 `requests_dispatched_rate`。

- FlexVol Volume 需要 Aggregate 參數、否則不需要。

- 。 `snapshot-policy` 參數必須設定為無。如此可確保不會意外還原快照、導致目前事件遺失、並防止可能的重複事件處理。

  如果您想要使用現有的空白磁碟區、請使用 `volume show` 命令來尋找它和 `volume modify` 命令進行任何必要的變更。確保原則、大小和 `snapshot-policy` 持續儲存區的參數已正確設定。

2. 建立持續儲存區：

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

   - 。 `vserver` 參數是 SVM 的名稱。
   - 。 `persistent-store` 參數是持續儲存區的名稱。
   - 。 `volume` 參數是持續儲存區磁碟區的名稱。

3. 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 ONTAP FPolicy 策略

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。

開始之前

- 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 ONTAP 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。

開始之前

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 ONTAP FPolicy 策略

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。

開始之前

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
```

版權資訊

商標資訊