Erstellen Sie die FPolicy-Konfiguration

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

Erstellen Sie die FPolicy-Konfiguration

Erstellen Sie die externe FPolicy Engine

Sie müssen eine externe Engine erstellen, um mit der Erstellung einer FPolicy-Konfiguration zu beginnen. Die externe Engine definiert, wie FPolicy Verbindungen zu externen FPolicy-Servern macht und managt. Wenn Ihre Konfiguration die interne ONTAP Engine (die native externe Engine) für einfaches Blockieren von Dateien verwendet, müssen Sie keine separate FPolicy externe Engine konfigurieren und müssen diesen Schritt nicht ausführen.

Was Sie benötigen

Der "Externer Motor" Arbeitsblatt sollte ausgefüllt werden.

Über diese Aufgabe

Wenn die externe Engine in einer MetroCluster-Konfiguration verwendet wird, sollten Sie die IP-Adressen der FPolicy-Server am Quellstandort als primäre Server angeben. Die IP-Adressen der FPolicy-Server am Zielstandort sollten als sekundäre Server angegeben werden.

Schritte

1. Erstellen Sie die FPolicy-externe Engine mit dem `vserver fpolicy policy external-engine create` Befehl.

   Mit dem folgenden Befehl wird eine externe Engine auf der Storage Virtual Machine (SVM) vs1.example.com erstellt. Für die externe Kommunikation mit dem FPolicy-Server ist keine Authentifizierung erforderlich.

   ```
   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. Überprüfen Sie die Konfiguration der externen FPolicy-Engine mit dem `vserver fpolicy policy external-engine show` Befehl.

   Mit dem folgenden Befehl werden Informationen zu allen auf SVM vs1.example.com konfigurierten externen Engines angezeigt:

   ```
   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
```

Mit dem folgenden Befehl werden ausführliche Informationen zur externen Engine mit dem Namen „`Engine1`“ auf SVM vs1.example.com angezeigt:

```
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: -
```

Erstellen Sie das FPolicy-Ereignis

Wenn Sie eine FPolicy-Konfiguration erstellen, müssen Sie ein FPolicy-Ereignis erstellen. Sie verknüpfen das Ereignis mit der FPolicy, wenn es erstellt wird. Ein Ereignis definiert, welches Protokoll überwacht werden soll und welche Dateizugriffsereignisse überwacht und gefiltert werden müssen.

Bevor Sie beginnen

Füllen Sie das FPolicy Event-Arbeitsblatt aus.

Schritte

1. Erstellen Sie das FPolicy-Ereignis mit `vserver fpolicy policy event create` Befehl.

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

2. Überprüfen Sie die FPolicy-Event-Konfiguration mit `vserver fpolicy policy event show` Befehl.

```
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
```

Erstellen Sie die FPolicy

Wenn Sie die FPolicy erstellen, verknüpfen Sie eine externe Engine und ein oder mehrere Ereignisse mit der Richtlinie. Die Richtlinie legt außerdem fest, ob ein obligatorisches Screening erforderlich ist, ob die FPolicy Server privilegierten Zugriff auf Daten auf der Storage Virtual Machine (SVM) haben und ob Passthrough-Read für Offline-Dateien aktiviert ist.

Was Sie benötigen

- Das Arbeitsblatt für die FPolicy sollte ausgefüllt werden.
- Wenn Sie planen, die Richtlinie für FPolicy-Server zu konfigurieren, muss die externe Engine vorhanden sein.
- Mindestens ein FPolicy-Ereignis, das Sie auf eine Verknüpfung mit der FPolicy planen, muss existieren.
- Wenn Sie einen privilegierten Datenzugriff konfigurieren möchten, muss auf der SVM ein SMB-Server vorhanden sein.

Schritte

1. Erstellen der FPolicy:

   ```
   vserver fpolicy policy create -vserver-name vserver_name -policy-name
   policy_name -engine engine_name -events event_name,… [-is-mandatory
   {true|false}] [-allow-privileged-access {yes|no}] [-privileged-user-name
   domain\user_name] [-is-passthrough-read-enabled {true|false}]
   ```

   - Sie können ein oder mehrere Events zur FPolicy hinzufügen.
   - Standardmäßig ist das obligatorische Screening aktiviert.
   - Wenn Sie privilegierten Zugriff zulassen möchten, setzen Sie die ein `-allow-privileged-access` Parameter an `yes`, Sie müssen auch einen privilegierten Benutzernamen für privilegierten Zugriff konfigurieren.
   - Wenn Sie Passthrough-read konfigurieren möchten, indem Sie die einstellen `-is-passthrough -read-enabled` Parameter an `true`, Sie müssen auch privilegierten Datenzugriff konfigurieren.

     Mit dem folgenden Befehl wird eine Richtlinie mit dem Namen „`policy1`“ erstellt, in der das Ereignis „`event1`“ und die externe Engine „`Engine1`“ mit ihr verknüpft sind. Diese Richtlinie verwendet Standardwerte in der Richtlinienkonfiguration: `vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

Mit dem folgenden Befehl wird eine Richtlinie mit dem Namen „policy2“ erstellt, in der das Ereignis „event2“ und die externe Engine „Engine2“ mit ihr verknüpft sind. Diese Richtlinie wurde für die Verwendung von privilegiertem Zugriff unter Verwendung des angegebenen Benutzernamens konfiguriert. Passthrough-read ist aktiviert:

```
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
```

Mit dem folgenden Befehl wird eine Richtlinie mit dem Namen „nativ1“ erstellt, die das Ereignis „event3“ mit ihr verknüpft hat. Diese Richtlinie verwendet die native Engine und verwendet Standardwerte in der Richtlinienkonfiguration:

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

2. Überprüfen Sie die FPolicy-Konfiguration mit `vserver fpolicy policy show` Befehl.

   Mit dem folgenden Befehl werden Informationen zu den drei konfigurierten FPolicy-Richtlinien angezeigt, einschließlich der folgenden Informationen:

   - Der Richtlinie zugeordnete SVM
   - Die externe Engine, die der Richtlinie zugeordnet ist
   - Die mit der Richtlinie verbundenen Ereignisse
   - Gibt an, ob eine obligatorische Überprüfung erforderlich ist
   - Gibt an, ob ein privilegierter Zugriff erforderlich ist `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
```

Erstellen Sie den FPolicy-Bereich

Nachdem Sie die FPolicy erstellt haben, müssen Sie einen FPolicy-Bereich erstellen. Bei der Erstellung des Anwendungsbereichs verknüpfen Sie den Geltungsbereich mit einer FPolicy. Ein Geltungsbereich definiert die Grenzen, für die die FPolicy gilt. Scopes können Dateien einschließen oder ausschließen, die auf Freigaben, Exportrichtlinien, Volumes und Dateierweiterungen basieren.

Was Sie benötigen

Das FPolicy Scope-Arbeitsblatt muss ausgefüllt werden. Die FPolicy muss mit einer zugeordneten externen Engine existieren (wenn die Richtlinie zur Verwendung externer FPolicy-Server konfiguriert ist) und über mindestens ein damit verbundener FPolicy-Ereignis verfügen.

Schritte

1. Erstellen Sie den FPolicy-Bereich mit `vserver fpolicy policy scope create` Befehl.

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

2. Überprüfen Sie die FPolicy-Scope-Konfiguration mit `vserver fpolicy policy scope show` Befehl.

   ```
   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: -
   ```

Aktivieren Sie die FPolicy

Nachdem Sie eine FPolicy-Konfiguration durchlaufen haben, aktivieren Sie die FPolicy. Durch das Aktivieren der Richtlinie wird die Priorität festgelegt und die Dateizugriffsüberwachung für die Richtlinie gestartet.

Was Sie benötigen

Die FPolicy muss mit einer zugeordneten externen Engine existieren (wenn die Richtlinie zur Verwendung externer FPolicy-Server konfiguriert ist) und über mindestens ein damit verbundener FPolicy-Ereignis verfügen. Der Richtlinienumfang von FPolicy muss vorhanden sein und der FPolicy zugewiesen werden.

Über diese Aufgabe

Die Priorität wird verwendet, wenn mehrere Richtlinien auf der Storage Virtual Machine (SVM) aktiviert sind und mehr als eine Richtlinie dasselbe Ereignis für den Dateizugriff abonniert hat. Richtlinien, die die native Engine-Konfiguration verwenden, haben für jede andere Engine eine höhere Priorität als Richtlinien, unabhängig von der ihnen bei der Aktivierung der Richtlinie zugewiesenen Sequenznummer.

Eine Richtlinie kann auf der Admin-SVM nicht aktiviert werden.

Schritte

1. Aktivieren Sie die FPolicy mithilfe von `vserver fpolicy enable` Befehl.

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

2. Überprüfen Sie, ob die FPolicy mit aktiviert wird `vserver fpolicy show` Befehl.

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

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