FPolicy 구성을 생성합니다

ONTAP 9

NetApp
April 24, 2024

목차

FPolicy 구성을 생성합니다

FPolicy 외부 엔진을 생성합니다

FPolicy 구성을 생성하려면 외부 엔진을 생성해야 합니다. 외부 엔진은 FPolicy가 외부 FPolicy 서버에 대한 연결을 만들고 관리하는 방법을 정의합니다. 구성에서 내부 ONTAP 엔진(기본 외부 엔진)을 간단한 파일 차단에 사용하는 경우 별도의 FPolicy 외부 엔진을 구성하지 않아도 되며 이 단계를 수행할 필요가 없습니다.

필요한 것

를 클릭합니다 "외부 엔진" 워크시트를 작성해야 합니다.

이 작업에 대해

외부 엔진이 MetroCluster 구성에 사용되는 경우 소스 사이트에 있는 FPolicy 서버의 IP 주소를 1차 서버로 지정해야 합니다. 대상 사이트에 있는 FPolicy 서버의 IP 주소를 2차 서버로 지정해야 합니다.

단계

1. 'vserver FPolicy external-engine create' 명령을 사용하여 FPolicy 외부 엔진을 생성합니다.

   다음 명령을 실행하면 SVM(스토리지 가상 시스템)vs1.example.com 에서 외부 엔진이 생성됩니다. FPolicy 서버와의 외부 통신에는 인증이 필요하지 않습니다.

   'vserver FPolicy external-engine create-vserver-name vs1.example.com -engine-name engine.1-primary-servers 10.1.1.2, 10.1.1.3-port 6789-SSL-option no-auth'

2. 'vserver FPolicy external-engine show' 명령을 사용하여 FPolicy 외부 엔진 구성을 확인하십시오.

   다음 명령을 실행하면 SVM vs1.example.com 에 구성된 모든 외부 엔진에 대한 정보가 표시됩니다.

   'vserver FPolicy policy external-engine show -vserver vs1.example.com'을 참조하십시오

```
                                Primary        Secondary
External
Vserver            Engine       Servers        Servers       Port Engine
Type
---------------    -----------  -------------- ----------- ------
-----------
vs1.example.com    engine1      10.1.1.2,      -             6789
synchronous
                                10.1.1.3
```

   다음 명령을 실행하면 SVM vs1.example.com 의 ""엔진1" 외부 엔진에 대한 자세한 정보가 표시됩니다.

   'vserver FPolicy policy external-engine show -vserver vs1.example.com -engine-name engine11'을 참조하십시오

```
                                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: -
```

FPolicy 이벤트를 생성합니다

FPolicy 정책 구성을 생성하는 과정에서 FPolicy 이벤트를 생성해야 합니다. 이벤트가 생성될 때 FPolicy 정책에 이벤트를 연결합니다. 이벤트는 모니터링하고 필터링할 파일 액세스 이벤트와 모니터링할 프로토콜을 정의합니다.

시작하기 전에

FPolicy 이벤트를 완료해야 합니다 "워크시트".

FPolicy 이벤트를 생성합니다

1. 'vserver FPolicy event create' 명령을 사용하여 FPolicy 이벤트를 생성합니다.

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

2. 'vserver FPolicy event show' 명령을 사용하여 FPolicy 이벤트 구성을 확인하십시오.

   'vserver FPolicy policy event show - vserver vs1.example.com'을 참조하십시오

   ```
                     Event                File                      Is Volume
   Vserver           Name      Protocols Operations    Filters   Operation
   ---------------   --------- --------- ------------- ---------
   ------------
   vs1.example.com   event1    cifs      open, close,  -         false
                                         read, write
   ```

FPolicy 액세스 거부 이벤트를 생성합니다

ONTAP 9.13.1 부터는 권한이 없어 실패한 파일 작업에 대한 알림을 받을 수 있습니다. 이러한 알림은 보안, 랜섬웨어 보호 및 거버넌스에 유용합니다.

1. 'vserver FPolicy event create' 명령을 사용하여 FPolicy 이벤트를 생성합니다.

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

영구 저장소를 만듭니다

ONTAP 9.14.1부터 FPolicy를 통해 를 설정할 수 있습니다 "영구 저장소" SVM에서 비동기적 정책에 대한 파일 액세스 이벤트를 캡처합니다. 영구 저장소는 클라이언트 I/O 처리를 FPolicy 알림 처리와 분리하여 클라이언트 지연 시간을 줄여 줍니다. 동기(필수 또는 비필수) 및 비동기 필수 구성은 지원되지 않습니다.

모범 사례

- 영구 저장소 기능을 사용하기 전에 파트너 응용 프로그램이 이 구성을 지원하는지 확인하십시오.
- 영구 저장소 볼륨은 SVM별로 설정됩니다. 각 FPolicy가 활성화된 SVM에 대해 영구 저장소 볼륨이 필요합니다.
- 영구 저장소 볼륨 이름과 볼륨 생성 시 지정된 접합 경로가 일치해야 합니다.
- Fpolicy에서 최대 트래픽을 모니터링할 것으로 예상되는 LIF로 노드에 영구 저장소 볼륨을 생성합니다.
- 스냅샷 정책을 로 설정합니다 `none` 에 대해 이야기해 보려고 합니다 `default`. 이는 스냅샷을 실수로 복구하여 현재 이벤트가 손실되지 않도록 하고 중복 이벤트 처리를 방지하기 위한 것입니다.
- 영구 저장소 볼륨을 외부 사용자 프로토콜 액세스(CIFS/NFS)에 액세스할 수 없도록 하여 영구 이벤트 레코드가 실수로 손상되거나 삭제되지 않도록 합니다. 이를 위해 FPolicy를 활성화한 후 ONTAP에서 볼륨을 마운트 해제하여 접합 경로를 제거하면 사용자 프로토콜 액세스에 액세스할 수 없게 됩니다.

단계

1. 영구 저장소용으로 프로비저닝할 수 있는 SVM에 빈 볼륨을 생성합니다.

   ```
   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>
   ```

   - 영구 저장소 볼륨의 크기는 외부 서버(파트너 응용 프로그램)에 전달되지 않은 이벤트를 유지할 기간을 기준으로 합니다.

     예를 들어, 초당 30,000개의 알림이 있는 클러스터에서 30분 이벤트를 지속하려는 경우:

     필요한 볼륨 크기 = 30000 x 30 x 60 x 0.6KB(평균 알림 레코드 크기) = 32400000KB = ~32GB

   대략적인 알림 비율을 확인하려면 FPolicy 파트너 애플리케이션에 문의하거나 FPolicy 카운터를 활용하십시오 `requests_dispatched_rate`.

   - 충분한 RBAC 권한(볼륨을 생성하기 위해)을 가진 관리자가 원하는 크기의 볼륨(volume CLI 명령 또는 REST API 사용)을 생성하고 해당 볼륨의 이름을 로 제공해야 합니다 `-volume` 영구 저장소에서 CLI 명령 또는 REST API를 생성합니다.

2. 영구 저장소 만들기:

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

- 영구 저장소: 영구 저장소 이름입니다
- 볼륨: 영구 저장소 볼륨입니다

3. 영구 저장소를 생성한 후 FPolicy 정책을 생성하고 영구 저장소 이름을 해당 정책에 추가할 수 있습니다. 자세한 내용은 을 참조하십시오 "FPolicy 정책을 생성합니다".

FPolicy 정책을 생성합니다

FPolicy 정책을 생성할 때 외부 엔진과 하나 이상의 이벤트를 정책에 연결합니다. 또한 이 정책은 필수 선별 작업이 필요한지 여부, FPolicy 서버가 SVM(스토리지 가상 머신)의 데이터에 액세스할 수 있는 권한이 있는지 여부 및 오프라인 파일에 대한 패스스루 읽기를 사용할 수 있는지 여부도 지정합니다.

필요한 것

- FPolicy 정책 워크시트를 작성해야 합니다.
- FPolicy 서버를 사용하도록 정책을 구성하려는 경우 외부 엔진이 존재해야 합니다.
- FPolicy 정책과 연관하려는 FPolicy 이벤트가 하나 이상 있어야 합니다.
- 특별 권한 데이터 액세스를 구성하려면 SVM에 SMB 서버가 있어야 합니다.
- 정책에 대한 영구 저장소를 구성하려면 엔진 유형이 * 비동기 * 여야 하고 정책이 * 비필수 * 여야 합니다.

  자세한 내용은 을 참조하십시오 "영구 저장소를 만듭니다".

단계

1. FPolicy 정책을 생성합니다.

```
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}]
```

   - FPolicy 정책에 하나 이상의 이벤트를 추가할 수 있습니다.
   - 기본적으로 필수 스크리닝이 활성화됩니다.
   - '-allow-privileged-access' 파라미터를 'yes'로 설정하여 권한 있는 액세스를 허용하려면 권한 있는 액세스에 대한 권한 있는 사용자 이름도 구성해야 합니다.
   - '-is-passthrough-read-enabled' 매개 변수를 'true'로 설정하여 패스스루 읽기를 구성하려면 권한이 있는 데이터 액세스도 구성해야 합니다.

     다음 명령을 실행하면 이벤트1, 외부 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진1 등의 정책1이 생성됩니다. 이 정책은 정책 구성에서 'vserver FPolicy policy create - vserver vs1.example.com -policy -name policy1 -events event1 - engine engine 1'이라는 기본값을 사용합니다

     다음 명령을 실행하면 이벤트2, 외부 엔진 등의 정책2가 생성됩니다. 이 정책은 지정된 사용자 이름을 사용하여 권한 있는 액세스를 사용하도록 구성됩니다. 패스스루 읽기가 활성화된 경우:

'vserver FPolicy policy create - vserver vs1.example.com - policy -name policy2 - event2 - event2 - engine engine 2 - allow-privileged-access yes-privileged-user-name example\archive_acct-is-passthrough-read-enabled true'

다음 명령은 ""event3""이라는 이벤트가 연결된 ""네이티브e1""이라는 정책을 만듭니다. 이 정책은 네이티브 엔진을 사용하며 정책 구성에서 기본값을 사용합니다.

'vserver FPolicy policy create-vserver vs1.example.com -policy-name naive1-event3-engine native'

2. 'vserver FPolicy show' 명령을 사용하여 FPolicy 정책 구성을 확인하십시오.

   다음 명령을 실행하면 다음 정보를 비롯하여 세 가지 구성된 FPolicy 정책에 대한 정보가 표시됩니다.

   - 정책과 연결된 SVM
   - 정책과 연결된 외부 엔진입니다
   - 정책과 관련된 이벤트입니다
   - 필수 스크리닝이 필요한지 여부
   - 특별 권한 액세스가 'vserver FPolicy show'인지 여부

```
   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
```

FPolicy 범위를 생성합니다

FPolicy 정책을 생성한 후에는 FPolicy 범위를 생성해야 합니다. 범위를 생성할 때 범위를 FPolicy 정책과 연계합니다. 범위는 FPolicy 정책이 적용되는 경계를 정의합니다. 범위에는 공유, 엑스포트 정책, 볼륨, 파일 확장명을 기준으로 파일을 포함하거나 제외할 수 있습니다.

필요한 것

FPolicy 범위 워크시트를 작성해야 합니다. FPolicy 정책은 연결된 외부 엔진과 함께 있어야 하며(정책이 외부 FPolicy 서버를 사용하도록 구성된 경우) 하나 이상의 관련 FPolicy 이벤트가 있어야 합니다.

단계

1. 'vserver FPolicy scope create' 명령을 사용하여 FPolicy 범위를 생성합니다.

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

2. 'vserver FPolicy scope show' 명령을 사용하여 FPolicy 범위 구성을 확인하십시오.

   'vserver FPolicy 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: -
```

FPolicy 정책을 사용합니다

FPolicy 정책 구성을 수행한 후 FPolicy 정책을 사용하도록 설정합니다. 정책을 설정하면 우선 순위가 설정되고 정책에 대한 파일 액세스 모니터링이 시작됩니다.

필요한 것

FPolicy 정책은 연결된 외부 엔진과 함께 있어야 하며(정책이 외부 FPolicy 서버를 사용하도록 구성된 경우) 하나 이상의 관련 FPolicy 이벤트가 있어야 합니다. FPolicy 정책 범위가 존재하며 FPolicy 정책에 할당해야 합니다.

이 작업에 대해

우선 순위는 SVM(스토리지 가상 시스템)에서 여러 정책이 활성화되어 있고 둘 이상의 정책이 동일한 파일 액세스 이벤트에 가입되어 있는 경우에 사용됩니다. 네이티브 엔진 구성을 사용하는 정책은 정책을 설정할 때 할당된 시퀀스 번호에 관계없이 다른 엔진에 대한 정책보다 우선 순위가 높습니다.

> 관리 SVM에서 정책을 활성화할 수 없습니다.

단계

1. 'vserver FPolicy enable' 명령을 사용하여 FPolicy 정책을 활성화하십시오.

   'vserver FPolicy enable-vserver-name vs1.example.com - policy-name policy1-sequence-number 1'

2. 'vserver FPolicy show' 명령을 사용하여 FPolicy 정책이 활성화되어 있는지 확인하십시오.

   'vserver FPolicy show -vserver vs1.example.com'을 참조하십시오

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