FPolicy設定の作成

ONTAP 9

NetApp
December 20, 2024

目次

FPolicy設定の作成

FPolicy外部エンジンの作成

FPolicy設定の作成を開始するには、外部エンジンを作成する必要があります。外部エンジンは、FPolicyが外部FPolicyサーバへの接続を確立および管理する方法を定義します。内部のONTAPエンジン（標準の外部エンジン）を単純なファイルブロッキングに使用している設定の場合は、FPolicy外部エンジンを別途設定する必要はなく、この手順を実行する必要もありません。

必要なもの

"外部エンジン"ワークシートを完成させる必要があります。

タスクの内容

外部エンジンがMetroCluster設定で使用されている場合は、ソースサイトでFPolicyサーバのIPアドレスをプライマリサーバとして指定する必要があります。デスティネーションサイトのFPolicyサーバのIPアドレスは、セカンダリサーバとして指定する必要があります。

手順

1. コマンドを使用してFPolicy外部エンジンを作成し `vserver fpolicy policy external-engine create`ます。

   次のコマンドは、Storage Virtual Machine（SVM）vs1.example.com上に外部エンジンを作成します。FPolicyサーバとの外部通信に認証は必要ありません。

   ```
   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. コマンドを使用してFPolicy外部エンジンの設定を確認します `vserver fpolicy policy external-engine show`。

   次のコマンドは、SVM vs1.example.comで設定されているすべての外部エンジンに関する情報を表示します。

   ```
   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
   ```

次のコマンドは、 SVM vs1.example.com 上の「 engine1 」という外部エンジンに関する詳細情報を表示します。

```
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: -
```

FPolicyイベントの作成

FPolicyポリシーの設定を作成する手順の一環として、FPolicyイベントを作成する必要があります。FPolicyポリシーの作成時にイベントを関連付けます。イベントは、監視するプロトコルと、監視およびフィルタリングするファイルアクセスイベントを定義します。

開始する前に

FPolicyイベントを完了する必要があります"ワークシート"。

FPolicyイベントの作成

1. コマンドを使用してFPolicyイベントを作成し `vserver fpolicy policy event create`ます。

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

2. コマンドを使用してFPolicyイベントの設定を確認します `vserver fpolicy policy event show`。

   ```
   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
   ```

FPolicyアクセス拒否イベントを作成する

ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。これらの通知は、セキュリティ、ランサムウェア対策、ガバナンスに役立ちます。

1. コマンドを使用してFPolicyイベントを作成し `vserver fpolicy policy event create`ます。

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

FPolicy永続的ストアの作成

永続的ストアを使用すると、クライアントI/O処理とFPolicy通知処理を分離して、クライアントのレイテンシを低減できます。14.1以降では、ONTAP 9の必須ではない非同期ポリシーのファイルアクセスイベントをキャプチャするようにを設定でき"永続的ストア"ます。同期（必須または非必須）および非同期の必須構成はサポートされていません。

ONTAP 9 .15.1以降では、FPolicyの永続的ストアの設定が簡素化されています。 `persistent-store create`コマンドは、SVM用のボリュームの作成を自動化し、永続的ストア用のボリュームを設定します。

永続ストアを作成するには、ONTAPのリリースに応じて次の2つの方法があります。

- ONTAP 9.15.1以降：永続ストアを作成すると、ONTAPでボリュームが自動的に作成されて設定されます。これにより、FPolicyの永続的ストアの設定が簡素化され、すべてのベストプラクティスが実装されます。
- ONTAP 9.14.1：ボリュームを手動で作成して設定し、新しく作成したボリューム用の永続的ストアを作成します。

各SVMに設定できる永続的ストアは1つだけです。ポリシーが別 々 のパートナーのものであっても、この単一の永続的ストアをそのSVM上のすべてのFPolicy設定に使用する必要があります。

永続ストアの作成（ONTAP 9 .15.1以降）

開始する前に

- 永続的ストアを作成するSVMには、アグリゲートが少なくとも1つ必要です。
- SVMで使用可能なアグリゲートへのアクセスと、ボリュームを作成するための十分な権限が必要です。

手順

1. 永続的ストアを作成します。これにより、ボリュームが自動的に作成および設定されます。

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

   - `vserver`パラメータは、SVMの名前です。
   - `persistent-store`パラメータは、永続ストアの名前です。
   - `volume`パラメータは、永続的ストアボリュームの名前です。

既存の空のボリュームを使用する場合は、コマンドを使用してボリューム `volume show`を検索し、volumeパラメータで指定します。

- この `size`パラメータは、外部サーバ（パートナーアプリケーション）に配信されないイベントを保持する期間に基づいています。

  たとえば、1秒あたり30Kの通知があるクラスタで30分間のイベントを維持する場合は、次のコマンドを実行します。

  必要なボリュームサイズ= 30000 x 30 x 60 x 0.6KB（通知レコードの平均サイズ）= 32400000 KB =~32GB

  おおよその通知速度を確認するには、FPolicyパートナーアプリケーションに連絡するか、FPolicyカウンタを利用します `requests_dispatched_rate`。

既存のボリュームを使用する場合、sizeパラメータはオプションです。sizeパラメータに値を指定すると、指定したサイズに一致するボリュームが変更されます。

- パラメータは `autosize-mode`、ボリュームのオートサイズモードを指定します。サポートされるオートサイズモードは次のとおりです。
  - off -使用済みスペースの量に応じてボリュームのサイズが拡張または縮小されません。
  - grow -ボリュームの使用済みスペースが拡張しきい値を超えると、ボリュームは自動的に拡張されます。
  - grow_shrink -使用済みスペースの量に応じてボリュームのサイズが拡張または縮小されます。

2. FPolicyポリシーを作成し、そのポリシーに永続ストア名を追加します。詳細については、を参照してください "FPolicyポリシーを作成する"。

永続ストアの作成（ONTAP 9 .14.1）

ボリュームを作成し、そのボリュームを使用する永続的ストアを作成できます。作成したボリュームを外部ユーザプロトコルアクセス（CIFS / NFS）からブロックできます。

手順

1. 永続ストア用にプロビジョニング可能な空のボリュームをSVMに作成します。

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

十分なRBAC Privileges（ボリュームの作成）を持つ管理者ユーザは、必要なサイズのボリュームを（volume CLIコマンドまたはREST APIを使用して）作成し、永続的ストアのcreate CLIコマンドまたはREST APIでとしてボリュームの名前を指定する必要があります `-volume`。

- `vserver`パラメータは、SVMの名前です。
- `volume`パラメータは、永続的ストアボリュームの名前です。
- ボリュームを使用できるようにするには、 `state`パラメータをonlineに設定する必要があります。
- `policy`FPolicyサービスポリシーをすでに設定している場合、パラメータはに設定されます。そう

でない場合は、あとでコマンドを使用してポリシーを追加できます `volume modify`。

- `unix-permissions`パラメータはオプションです。
- この `size`パラメータは、外部サーバ（パートナーアプリケーション）に配信されないイベントを保持する期間に基づいています。

  たとえば、1秒あたり30Kの通知があるクラスタで30分間のイベントを維持する場合は、次のコマンドを実行します。

  必要なボリュームサイズ= 30000 x 30 x 60 x 0.6KB（通知レコードの平均サイズ）= 32400000 KB =~32GB

おおよその通知速度を確認するには、FPolicyパートナーアプリケーションに連絡するか、FPolicyカウンタを利用します `requests_dispatched_rate`。

- FlexVolボリュームの場合はaggregateパラメータが必要です。それ以外の場合は必須ではありません。
- `snapshot-policy`パラメータはnoneに設定する必要があります。これにより、スナップショットが誤ってリストアされて現在のイベントが失われることがなくなり、イベント処理の重複を防ぐことができます。

  既存の空のボリュームを使用する場合は、コマンドを使用してボリュームを検索し、コマンドを使用し `volume show`て必要な変更を行います。 `volume modify`永続ストアのポリシー、サイズ、およびパラメータが正しく設定されていることを確認します `snapshot-policy`。

2. 永続ストアを作成します。

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

   - `vserver`パラメータは、SVMの名前です。
   - `persistent-store`パラメータは、永続ストアの名前です。
   - `volume`パラメータは、永続的ストアボリュームの名前です。

3. FPolicyポリシーを作成し、そのポリシーに永続ストア名を追加します。詳細については、を参照してください "FPolicyポリシーを作成する"。

FPolicyポリシーを作成する

FPolicyポリシーを作成するときは、外部エンジンと1つ以上のイベントをポリシーに関連付けます。また、このポリシーでは、必須のスクリーニングが必要かどうか、FPolicyサーバにStorage Virtual Machine（SVM）上のデータへの権限付きアクセスが許可されているかどうか、オフラインファイルのパススルーリードが有効かどうかを指定します。

必要なもの

- FPolicyポリシーワークシートを完成させる必要があります。
- FPolicyサーバを使用するようにポリシーを設定する場合は、外部エンジンが存在している必要があります。

- FPolicyポリシーに関連付けるFPolicyイベントが少なくとも1つ存在している必要があります。
- 権限付きデータアクセスを設定する場合は、SVM上にSMBサーバが存在している必要があります。
- ポリシーの永続ストアを設定するには、エンジンタイプを* async にし、ポリシーを non-mandatory *にする必要があります。

  詳細については、を参照してください "永続ストアの作成"。

手順

1. FPolicyポリシーを作成します。

   ```
   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 ポリシーには 1 つ以上のイベントを追加できます。
   - デフォルトでは、必須のスクリーニングが有効になっています。
   - パラメータをに `yes`設定して権限付きアクセスを許可する場合 `-allow-privileged-access`は、権限付きアクセスの権限付きユーザ名も設定する必要があります。
   - パラメータをに `true`設定してパススルーリードを設定する場合 `-is-passthrough-read-enabled`は、権限付きデータアクセスも設定する必要があります。

     次のコマンドは、 "event1" というイベントと、 "engine1" という外部エンジンが関連付けられた "policy1 " という名前のポリシーを作成します。このポリシーでは、ポリシー設定にデフォルト値を使用します。 `vserver fpolicy policy create -vserver vs1.example.com -policy -name policy1 -events event1 -engine engine1`

     次のコマンドは、 "event2`" というイベントと、 "engine2`" という外部エンジンが関連付けられた "policy2`" というポリシーを作成します。このポリシーは、指定したユーザ名を使用して権限付きアクセスを使用するように設定されています。パススルーリードが有効になっている場合：

     ```
     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
     ```

     次のコマンドは ' event3` というイベントが関連付けられた ' ' native1` という名前のポリシーを作成しますこのポリシーでは標準のエンジンを使用し、デフォルト値をポリシー設定に使用します。

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

2. コマンドを使用してFPolicyポリシーの設定を確認します `vserver fpolicy policy show`。

   次のコマンドは、次の情報を含む、設定された3つのFPolicyポリシーに関する情報を表示します。

   - ポリシーに関連付けられている SVM
   - ポリシーに関連付けられている外部エンジン

- ポリシーに関連付けられているイベント
- スクリーニングを必須にするかどうか
- 権限付きアクセスが必要かどうか `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
```

FPolicyスコープを作成する

FPolicy ポリシーを作成したら、 FPolicy スコープを作成する必要があります。スコープを作成するときに、スコープを FPolicy ポリシーに関連付けます。スコープは、FPolicy ポリシーが適用される範囲を定義します。共有、エクスポートポリシー、ボリューム、およびファイル拡張子に基づいて、対象とするファイルまたは除外するファイルを指定できます。

必要なもの

FPolicy スコープワークシートを完成させる必要があります。FPolicy ポリシーには、関連付けられた外部エンジンが存在する必要があり（外部 FPolicy サーバを使用するようにポリシーを設定する場合）、 FPolicy イベントを少なくとも 1 つは関連付ける必要があります。

手順

1. コマンドを使用してFPolicyスコープを作成し `vserver fpolicy policy scope create`ます。

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

2. コマンドを使用してFPolicyスコープの設定を確認します `vserver fpolicy policy scope show`。

   ```
   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: -
```

FPolicyポリシーを有効にする

FPolicy ポリシーの設定が完了したら、 FPolicy ポリシーを有効にします。ポリシーを有効にすると、優先度が設定され、ポリシーのファイルアクセスの監視が開始されます。

必要なもの

FPolicy ポリシーには、関連付けられた外部エンジンが存在する必要があり（外部 FPolicy サーバを使用するようにポリシーを設定する場合）、 FPolicy イベントを少なくとも 1 つは関連付ける必要があります。FPolicy ポリシースコープが存在し、 FPolicy ポリシーに割り当てられている必要があります。

タスクの内容

Storage Virtual Machine（SVM）で複数のポリシーを有効にし、複数のポリシーを同じファイルアクセスイベントに登録している場合は、優先度が使用されます。標準のエンジン設定を使用するポリシーは、ポリシーを有効にするときに割り当てられたシーケンス番号に関係なく、他のエンジンのポリシーよりも優先度が高くなります。

管理 SVM ではポリシーを有効にできません。

手順

1. コマンドを使用して、FPolicyポリシーを有効にし `vserver fpolicy enable`ます。

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

2. コマンドを使用して、FPolicyポリシーが有効になっていることを確認します `vserver fpolicy show`。

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

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

著作権に関する情報

商標に関する情報