创建 FPolicy 配置

ONTAP 9

NetApp
April 24, 2024

目录

创建 FPolicy 配置

创建 FPolicy 外部引擎

您必须创建外部引擎才能开始创建 FPolicy 配置。外部引擎定义了 FPolicy 如何建立和管理与外部 FPolicy 服务器的连接。如果您的配置使用内部 ONTAP 引擎（原生外部引擎）来简单地阻止文件，则无需配置单独的 FPolicy 外部引擎，也无需执行此步骤。

您需要的内容

。 "外部引擎" 应填写工作表。

关于此任务

如果在 MetroCluster 配置中使用外部引擎，则应将源站点上 FPolicy 服务器的 IP 地址指定为主服务器。目标站点上 FPolicy 服务器的 IP 地址应指定为二级服务器。

步骤

1. 使用创建FPolicy外部引擎 `vserver fpolicy policy external-engine create` 命令：

   以下命令将在 Storage Virtual Machine （ SVM ） vs1.example.com 上创建外部引擎。与 FPolicy 服务器的外部通信不需要身份验证。

   ```
   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. 使用验证FPolicy外部引擎配置 `vserver fpolicy policy external-engine show` 命令：

   以下命令显示有关在 SVM vs1.example.com 上配置的所有外部引擎的信息：

   ```
   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
   ```

   以下命令显示有关 SVM vs1.example.com 上名为 "`Engine1` " 的外部引擎的详细信息：

   ```
   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: -
```

创建 FPolicy 事件

在创建 FPolicy 策略配置过程中，您需要创建 FPolicy 事件。您可以在创建事件时将其与 FPolicy 策略相关联。事件定义要监控的协议以及要监控和筛选的文件访问事件。

开始之前

您应完成FPolicy事件 "工作表"。

创建 FPolicy 事件

1. 使用创建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. 使用验证FPolicy事件配置 `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
   ```

创建FPolicy拒绝访问事件

从ONTAP 9.13.1开始、用户可以收到因缺少权限而导致文件操作失败的通知。这些通知对于安全性、勒索软件防护和监管非常重要。

1. 使用创建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
```

创建持久性存储

从ONTAP 9.14.1开始、FPolicy允许您设置 "永久性存储" 捕获SVM中异步非强制策略的文件访问事件。永久性存储有助于将客户端I/O处理与FPolicy通知处理分离、以减少客户端延迟。不支持同步(强制或非强制)和异步强制配置。

最佳实践

- 在使用永久性存储功能之前、请确保您的合作伙伴应用程序支持此配置。
- 永久性存储卷会按SVM进行设置。对于启用了FPolicy的每个SVM、您都需要一个永久性存储卷。
- 创建卷时指定的永久性存储卷名称和接合路径应匹配。
- 在包含预期Fpolicy监控的最大流量的生命周期的节点上创建永久性存储卷。
- 将Snapshot策略设置为 `none` 而不是 `default`。这是为了确保不会意外还原快照而导致当前事件丢失、并防止可能发生重复的事件处理。
- 使持久存储卷无法用于外部用户协议访问(CIFS或NFS)、以避免意外损坏或删除保留的事件记录。为此、在启用FPolicy后、请在ONTAP中卸载卷以删除接合路径、这样用户协议访问就无法访问该路径。

步骤

1. 在SVM上创建一个可为永久性存储配置的空卷：

   ```
   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>
   ```

   - 永久性存储卷的大小取决于您要使未传送到外部服务器(配对应用程序)的事件持久化的持续时间。

     例如、如果您希望在每秒容量为3万次通知的集群中持久保留30分钟的事件：

     所需卷大小= 30000 x 30 x 60 x 0.6 KB (平均通知记录大小)= 3240000 KB =~32 GB

   要了解大致的通知率、您可以联系您的FPolicy合作伙伴申请、也可以使用FPolicy计数器 `requests_dispatched_rate`。

   - 具有足够RBAC权限(用于创建卷)的管理员用户应使用volume CLI命令或REST API创建所需大小的卷、并将该卷的名称提供为 `-volume` 在永久性存储中、创建CLI命令或REST API。

2. 创建永久性存储：

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

   - 永久性存储：永久性存储名称
   - volume：永久性存储卷

3. 创建永久性存储后、您可以创建FPolicy策略并将此永久性存储名称添加到该策略中。 有关详细信息，请参见 "创建 FPolicy 策略"。

创建 FPolicy 策略

创建 FPolicy 策略时，您需要将一个外部引擎以及一个或多个事件与此策略相关联。该策略还指定是否需要强制筛选， FPolicy 服务器是否有权访问 Storage Virtual Machine （ SVM ）上的数据，以及是否已启用对脱机文件的直通读取。

您需要的内容

- 应填写 FPolicy 策略工作表。
- 如果您计划配置策略以使用 FPolicy 服务器，则外部引擎必须存在。
- 您计划与 FPolicy 策略关联的至少一个 FPolicy 事件必须存在。
- 如果要配置有权限的数据访问、SVM上必须存在SMB服务器。
- 要为策略配置永久性存储，引擎类型必须为*async*，策略必须为*non-man强制*。

  有关详细信息，请参见 "创建持久性存储"。

步骤

1. 创建 FPolicy 策略：

   ```
   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}]
   ```

   - 您可以将一个或多个事件添加到 FPolicy 策略中。
   - 默认情况下，强制筛选处于启用状态。
   - 如果要通过设置来允许特权访问 `-allow-privileged-access` 参数设置为 `yes`，您还必须为特权访问配置特权用户名。
   - 如果要通过设置来配置直通读取 `-is-passthrough-read-enabled` 参数设置为 `true`，您还必须配置有权限的数据访问。

     以下命令将创建一个名为 "`policy1` " 的策略，该策略会将事件命名为 "`EVENT1` " ，并将外部引擎命名为 "`Engine1` " 。此策略在策略配置中使用默认值： `vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

     以下命令将创建一个名为 "`policy2` " 的策略，其中包含名为 "`event2` " 的事件以及名为 "`engine2` " 的外部引擎。此策略配置为使用指定的用户名进行特权访问。已启用直通读取：

     ```
     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
     ```

     以下命令将创建一个名为 "`native1` " 的策略，该策略与名为 "`event3` " 的事件关联。此策略使用原生引擎并在策略配置中使用默认值：

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

2. 使用验证FPolicy策略配置 `vserver fpolicy policy show` 命令：

   以下命令显示有关已配置的三个 FPolicy 策略的信息，其中包括以下信息：

   - 与策略关联的 SVM
   - 与策略关联的外部引擎
   - 与策略关联的事件
   - 是否需要强制筛查
   - 是否需要特权访问 `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
```

创建 FPolicy 范围

创建 FPolicy 策略后，您需要创建 FPolicy 范围。在创建范围时，您可以将此范围与 FPolicy 策略相关联。范围用于定义适用 FPolicy 策略的边界。范围可以根据共享，导出策略，卷和文件扩展名包括或排除文件。

您需要的内容

必须填写 FPolicy 范围工作表。FPolicy 策略必须与关联的外部引擎一起存在（如果将此策略配置为使用外部 FPolicy 服务器），并且必须至少具有一个关联的 FPolicy 事件。

步骤

1. 使用创建FPolicy范围 `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. 使用验证FPolicy范围配置 `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: -
```

启用 FPolicy 策略

配置完 FPolicy 策略配置后，可以启用 FPolicy 策略。启用此策略可设置其优先级并开始监控此策略的文件访问。

您需要的内容

FPolicy 策略必须与关联的外部引擎一起存在（如果将此策略配置为使用外部 FPolicy 服务器），并且必须至少具有一个关联的 FPolicy 事件。FPolicy 策略范围必须存在，并且必须分配给 FPolicy 策略。

关于此任务

如果在 Storage Virtual Machine （ SVM ）上启用了多个策略，并且多个策略已订阅同一文件访问事件，则会使用此优先级。对于任何其他引擎，使用原生引擎配置的策略的优先级都高于策略，无论启用策略时为其分配的序列号如何。

> 无法在管理 SVM 上启用策略。

步骤

1. 使用启用FPolicy策略 `vserver fpolicy enable` 命令：

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

2. 使用验证是否已启用FPolicy策略 `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
   ```