



创建 FPolicy 配置

ONTAP 9

NetApp
February 12, 2026

目录

创建 FPolicy 配置	1
创建 ONTAP FPolicy 外部引擎	1
创建 ONTAP FPolicy 事件	2
创建 FPolicy 事件	2
创建 FPolicy 拒绝访问事件	2
创建 ONTAP FPolicy 持久存储	3
创建永久性存储(ONTAP 9.151或更高版本)	3
创建永久性存储(ONTAP 9.14.1)	4
创建 ONTAP FPolicy 策略	5
创建 ONTAP FPolicy 范围	6
启用 ONTAP FPolicy 策略	7

创建 FPolicy 配置

创建 ONTAP 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。

开始之前

- “[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
```

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

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

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 ONTAP FPolicy 持久存储

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。从ONTAP 9.14.1开始、您可以使用FPolicy进行设置 "[永久性存储](#)" 捕获SVM中异步非强制策略的文件访问事件。不支持同步(强制或非强制)和异步强制配置。

从ONTAP 9.15.1开始、FPolicy持久存储配置得到了简化。。 `persistent-store create` 命令可自动为SVM创建卷、并为永久性存储配置卷。

根据ONTAP版本、可以通过两种方式创建永久性存储：

- ONTAP 9.151或更高版本：创建永久性存储时、ONTAP会同时自动创建和配置其卷。这样可以简化FPolicy持久存储配置并实施所有最佳实践。
- ONTAP 9.14.1：手动创建和配置卷、然后为新创建的卷创建永久性存储。

每个SVM上只能设置一个永久性存储。该SVM上的所有FPolicy配置都需要使用这一永久性存储、即使这些策略来自不同的合作伙伴也是如此。

创建永久性存储(ONTAP 9.151或更高版本)

从ONTAP 9.15.1开始、使用 `fpolicy persistent-store create` 命令以创建FPolicy持久存储并创建和配置实时卷。ONTAP会自动阻止卷访问外部用户协议(CIFS或NFS)。

开始之前

- 要创建永久性存储的SVM必须至少具有一个聚合。
- 您应有权访问可用于SVM的聚合、并具有足够的权限来创建卷。

步骤

1. 创建永久性存储、用于自动创建和配置卷：

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

- 。 `vserver` parameter是SVM的名称。
- 。 `persistent-store` parameter是永久性存储的名称。
- 。 `volume` 参数是永久性存储卷的名称。



如果要使用现有的空卷、请使用 `volume show` 命令以查找此卷并在`volume`参数中指定此卷。

- 。 `size` 参数基于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= $30000 \times 30 \times 60 \times 0.6 \text{ KB}$ (平均通知记录大小)= $3240000 \text{ KB} =\sim 32 \text{ GB}$

要查找大致的通知率，您可以联系您的FPolicy合作伙伴应用程序，也可以使用FPolicy计数器 requests_dispatched_rate。



如果您使用的是现有卷、则size参数是可选的。如果为size参数提供了值、则它将使用您指定的大小修改卷。

- 。 autosize-mode 参数用于指定卷的自动调整模式。支持的自动调整模式包括：
 - off—卷大小不会根据已用空间量而增长或缩减。
 - 增长—当卷中的已用空间超过增长阈值时、卷会自动增长。
 - shr增长_shrink—卷大小根据已用空间量而增大或缩小。

2. 创建FPolicy策略并将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](#)"。

创建永久性存储(ONTAP 9.14.1)

您可以创建一个卷、然后创建一个永久性存储以使用该卷。然后、您可以阻止外部用户协议访问(CIFS或NFS)新创建的卷。

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

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。

- 。 vserver parameter是SVM的名称。
- 。 volume 参数是永久性存储卷的名称。
- 。 state 参数应设置为联机、以便可以使用此卷。
- 。 policy 参数设置为FPolicy服务策略(如果已配置)。如果没有、则可以使用 volume modify 命令以添加策略。
- 。 unix-permissions 参数是可选的。
- 。 size 参数基于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= $30000 \times 30 \times 60 \times 0.6 \text{ KB}$ (平均通知记录大小)= $3240000 \text{ KB} =\sim 32 \text{ GB}$

要查找大致的通知率，您可以联系您的FPolicy合作伙伴应用程序，也可以使用FPolicy计数器 requests_dispatched_rate。

- FlexVol卷需要使用聚合参数、否则不需要此参数。

- 。 `snapshot-policy` 参数必须设置为`none`。这样可以确保不会意外还原快照、从而导致当前事件丢失、并防止可能发生重复的事件处理。

如果要使用现有的空卷、请使用 `volume show` 命令以查找它和 `volume modify` 命令进行任何必要的更改。确保策略、大小和 `snapshot-policy` 已为持久性存储正确设置参数。

2. 创建永久性存储：

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

- 。 `vserver` parameter是SVM的名称。
- 。 `persistent-store` parameter是永久性存储的名称。
- 。 `volume` 参数是永久性存储卷的名称。

3. 创建FPolicy策略并将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 ONTAP 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。

开始之前

- 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 Name	Events	Engine	Is Mandatory	Privileged 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 ONTAP 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。

开始之前

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 ONTAP 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。

开始之前

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
```

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

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。