规划 **FPolicy** 配置

ONTAP 9

NetApp
February 12, 2026

目录

规划 FPolicy 配置

配置 ONTAP FPolicy 的要求、注意事项和最佳实践

在 Storage Virtual Machine （ SVM ）上创建和配置 FPolicy 配置之前，您需要了解配置 FPolicy 的某些要求，注意事项和最佳实践。

FPolicy功能可通过命令行界面(CLI)或REST API进行配置。

设置 FPolicy 的要求

在 Storage Virtual Machine （ SVM ）上配置和启用 FPolicy 之前，您需要了解某些要求。

- 集群中的所有节点都必须运行支持 FPolicy 的 ONTAP 版本。
- 如果您不使用 ONTAP 原生 FPolicy 引擎，则必须安装外部 FPolicy 服务器（ FPolicy 服务器）。
- FPolicy 服务器必须安装在可从启用了 FPolicy 策略的 SVM 的数据 LIF 访问的服务器上。

> 从FPolicy.8开始、ONTAP除了为出站ONTAP 9连接提供客户端LIF服务外、还会添加此 `data-fpolicy-client`服务。"详细了解LIF和服务策略"(英文)

- 必须在 FPolicy 策略外部引擎配置中将 FPolicy 服务器的 IP 地址配置为主服务器或二级服务器。
- 如果 FPolicy 服务器通过有权限的数据通道访问数据，则必须满足以下附加要求：
  - SMB 必须在集群上获得许可。

    通过 SMB 连接实现有权限的数据访问。
  - 必须配置用户凭据才能通过有权限的数据通道访问文件。
  - FPolicy 服务器必须在 FPolicy 配置中配置的凭据下运行。
  - 必须将用于与FPolicy服务器通信的所有数据SIFs配置为具有 `cifs` 作为允许的协议之一。

    这包括用于直通读取连接的 LIF 。

设置 FPolicy 时的最佳实践和建议

在Storage Virtual Machine (SVM)上设置FPolicy时、请熟悉常规配置最佳实践和建议、以确保您的FPolicy配置提供稳定可靠的监控性能和结果、从而满足您的要求。

有关性能、规模估算和配置的具体准则、请使用您的FPolicy合作伙伴应用程序。

永久性存储

从ONTAP 9.14.1开始、您可以通过FPolicy设置永久性存储、以捕获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。

- 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。
- 对于启用了FPolicy的每个SVM、您需要一个永久性存储。
  - 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。
- ONTAP 9.151或更高版本：
  - 创建永久性存储时、系统会自动处理永久性存储及其卷和卷配置。
- ONTAP 9.14.1：
  - 永久性存储、其卷及其卷配置是手动处理的。
- 在包含预期FPolicy监控最大流量的生命周期的节点上创建永久性存储卷。
  - ONTAP 9.151或更高版本：在创建永久性存储期间自动创建和配置卷。
  - ONTAP 9.14.1：集群管理员需要在启用了FPolicy的每个SVM上为永久性存储创建和配置卷。
- 如果持久性存储中累积的通知超过所配置卷的大小、则FPolicy将开始删除传入通知并显示相应的EMS消息。
  - ONTAP 9.151或更高版本：以及 `size` 参数、 `autosize-mode` 参数可帮助卷根据已用空间量增长或缩减。
  - ONTAP 9.14.1： `size` 参数在卷创建期间进行配置、以提供最大限制。
- 将Snapshot策略设置为 `none` 用于永久性存储卷、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。
  - ONTAP 9.151或更高版本： `snapshot-policy` 在创建永久性存储期间、参数会自动配置为none。
  - ONTAP 9.14.1： `snapshot-policy` 参数配置为 `none` 创建卷期间。
- 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。
  - ONTAP 9.15.1或更高版本：创建永久性存储期间、ONTAP会自动阻止卷访问外部用户协议(CIFS)。
  - ONTAP 9.14.1：启用FPolicy后、在ONTAP中卸载卷以删除接合路径。这样、外部用户协议访问(CIFS或NFS)将无法访问它。

有关详细信息，请参见 "FPolicy持久存储" 和 "创建持久性存储"。

持久存储故障转移和恢复

持久存储将保持接收到最后一个事件、发生意外重新启动或FPolicy被禁用并再次启用时的状态。接管操作完成后、配对节点将存储和处理新事件。在执行了恢复操作之后、永久性存储将恢复处理节点接管发生后可能仍存在的任何未处理事件。实时事件的优先级高于不经过处理的事件。

如果持久存储卷从同一 SVM 中的一个节点移动到另一个节点，则尚未处理的通知也会移动到新节点。您需要重新运行 `fpolicy persistent-store create`移动卷后，在任一节点上执行命令，以确保待处理的通知传递到外部服务器。

详细了解 `fpolicy persistent-store create`在"ONTAP 命令参考" 。

策略配置

为SVM配置FPolicy外部引擎、事件和范围可以改善整体体验和安全性。

- 为SVM配置FPolicy外部引擎：
  - 提供额外的安全性会降低性能成本。启用安全套接字层(SSL)通信会影响访问共享的性能。
  - FPolicy外部引擎应配置多个FPolicy服务器、以提供FPolicy服务器通知处理的故障恢复能力和高可用性。
- 为SVM配置FPolicy事件：

  监控文件操作会影响您的整体体验。例如、在存储端筛选不需要的文件操作可以改善您的体验。NetApp建议设置以下配置：

  - 监控最小文件操作类型并启用最大数量的筛选器、而不会违反使用情形。
  - 对getattr、读取、写入、打开和关闭操作使用筛选器。SMB和NFS主目录环境中的这些操作所占比例较高。
- 配置SVM的FPolicy范围：

  将策略的范围限制为相关存储对象、例如共享、卷和导出、而不是在整个SVM中启用这些对象。NetApp建议检查目录扩展名。如果 `is-file-extension-check-on-directories-enabled` 参数设置为 `true` ，目录对象将与常规文件一样进行扩展名检查。

网络配置：

FPolicy服务器和控制器之间的网络连接应具有低延迟。NetApp建议使用专用网络将FPolicy流量与客户端流量分隔开。

此外、您还应将外部FPolicy服务器(FPolicy服务器)放置在具有高带宽连接的集群附近、以实现最低延迟和高带宽连接。

> 如果将用于FPolicy流量的LIF配置在与用于客户端流量的LIF不同的端口上、则FPolicy LIF可能会因端口故障而故障转移到另一节点。因此、无法从节点访问FPolicy服务器、从而导致节点上文件操作的FPolicy通知失败。要避免出现此问题描述、请验证是否可通过节点上的至少一个LIF访问FPolicy服务器、以处理对该节点执行文件操作的FPolicy请求。

硬件配置

您可以将FPolicy服务器放置在物理服务器或虚拟服务器上。如果FPolicy服务器位于虚拟环境中、则应为此虚拟服务器分配专用资源(CPU、网络和内存)。

应优化集群节点与 FPolicy 服务器比率，以确保 FPolicy 服务器不会过载，这可能会在 SVM 响应客户端请求时导致延迟。最佳比率取决于使用FPolicy服务器的配对应用程序。NetApp建议与合作伙伴合作确定适当的价值。

多策略配置

无论序列号如何、用于本机阻止的FPolicy策略都具有最高优先级、而决策策略的优先级高于其他策略。策略优先级取决于使用情形。NetApp建议与合作伙伴合作确定适当的优先级。

大小注意事项

FPolicy对SMB和NFS操作执行实时监控、向外部服务器发送通知并等待响应、具体取决于外部引擎通信模式(同步或异步)。此过程会影响SMB和NFS访问以及CPU资源的性能。

要缓解任何问题、NetApp建议在启用FPolicy之前与合作伙伴一起评估环境并对其进行规模估算。性能受多种因素影响、包括用户数量、工作负载特征(例如每个用户的操作数和数据大小)、网络延迟以及故障或服务器速度减低。

监控性能

FPolicy是一个基于通知的系统。通知将发送到外部服务器进行处理、并生成对ONTAP的响应。此往返过程会增加客户端访问的延迟。

通过监控FPolicy服务器和ONTAP中的性能计数器、您可以发现解决方案中的瓶颈、并根据需要调整参数以获得最佳解决方案。例如、FPolicy延迟的增加会对SMB和NFS访问延迟产生级联影响。因此、您应同时监控工作负载(SMB和NFS)和FPolicy延迟。此外、您还可以在ONTAP中使用服务质量策略为启用了FPolicy的每个卷或SVM设置工作负载。

NetApp建议运行 `statistics show -object workload` 命令以显示工作负载统计信息。此外、您还应监控以下参数：

- 平均、读取和写入时间
- 操作总数
- 读取和写入计数器

您可以使用以下FPolicy计数器监控FPolicy子系统的性能。

> 您必须处于诊断模式才能收集与FPolicy相关的统计信息。

步骤

1. 收集FPolicy计数器：
   a. `statistics start -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics start -object fpolicy_policy -instance <instance_name> -sample-id <ID>`
2. 显示FPolicy计数器：
   a. `statistics show -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics show -object fpolicy_server -instance <instance_name> -sample-id <ID>`

   。 `fpolicy` 和 `fpolicy_server` 计数器可提供有关下表中所述的多个性能参数的信息。

计数器	**Description**
fpolicy计数器	已中止请求
在SVM上中止处理的屏幕请求数量	event_count
生成通知的事件列表	max_request_延迟
最大屏幕请求延迟	未完成_请求

计数器	**Description**
正在处理的屏幕请求总数	processed_requests
在SVM上执行fpolicy处理的屏幕请求总数	Request_延迟 历史记录
屏幕请求延迟的直方图	Requests_发放 率
每秒发送的屏幕请求数	Requests_received_rate
每秒接收的屏幕请求数	**fpolicy_server counters**计数器
max_request_延迟	屏幕请求的最大延迟
未完成_请求	等待响应的屏幕请求总数
request_延迟	屏幕请求的平均延迟
Request_延迟 历史记录	屏幕请求延迟的直方图
Request_sent率	每秒发送到FPolicy服务器的屏幕请求数
respony_received_rate	每秒从FPolicy服务器收到的屏幕响应数

有关和的 `statistics show`详细信息 `statistics start`，请参见"ONTAP 命令参考"。

管理**FPolicy**工作流以及对其他技术的依赖

NetApp建议在进行任何配置更改之前禁用FPolicy策略。例如、如果要在为已启用策略配置的外部引擎中添加或修改某个IP地址、请先禁用该策略。

如果将FPolicy配置为监控NetApp FlexCache卷、NetApp建议您不要将FPolicy配置为监控读取和getATTR文件操作。在ONTAP中监控这些操作需要检索索引节点到路径(i2P)数据。由于无法从FlexCache卷检索I2P数据、因此必须从初始卷检索这些数据。因此、监控这些操作会消除FlexCache可提供的性能优势。

部署FPolicy和机下防病毒解决方案后、防病毒解决方案会首先收到通知。FPolicy处理仅在防病毒扫描完成后开始。正确估算防病毒解决方案的规模非常重要、因为速度较慢的防病毒扫描程序可能会影响整体性能。

直通读取升级和还原注意事项

在升级到支持直通读取的 ONTAP 版本之前或还原到不支持直通读取的版本之前，您必须了解某些升级和还原注意事项。

升级

在将所有节点升级到支持 FPolicy 直通读取的 ONTAP 版本后，集群可以使用直通读取功能；但是，在现有 FPolicy 配置中，直通读取默认处于禁用状态。要对现有 FPolicy 配置使用直通读取，必须禁用 FPolicy 策略并修改配置，然后重新启用配置。

还原

还原到不支持FPolicy直通读取的ONTAP版本之前、您必须满足以下条件：

- 使用直通读取禁用所有策略、然后修改受影响的配置、使其不使用直通读取。
- 通过禁用集群上的每个FPolicy策略、在集群上禁用FPolicy功能。

在还原到不支持永久性存储的ONTAP版本之前、请确保所有FPolicy策略均未配置永久性存储。如果配置了永久性存储、还原将失败。

相关信息

- "统计数据显示"
- "统计开始"

设置 ONTAP FPolicy 配置

要监控文件访问，必须先在需要 FPolicy 服务的 Storage Virtual Machine （ SVM ）上创建并启用 FPolicy 配置。

在 SVM 上设置和启用 FPolicy 配置的步骤如下：

1. 创建 FPolicy 外部引擎。

   FPolicy 外部引擎可识别与特定 FPolicy 配置关联的外部 FPolicy 服务器（ FPolicy 服务器）。如果使用内部 "`FPolicy` " 原生引擎创建原生文件阻止配置，则无需创建 FPolicy 外部引擎。

   从ONTAP 9.15.1开始、您可以使用 `protobuf` 引擎格式。设置为时 `protobuf`、通知消息使用Google Protobuf以二进制格式进行编码。将引擎格式设置为之前 `protobuf`下，请确保`FPolicy`服务器也支持 `protobuf` 反序列化。有关详细信息，请参见 "规划 FPolicy 外部引擎配置"

2. 创建 FPolicy 事件。

   FPolicy 事件描述了 FPolicy 策略应监控的内容。事件由要监控的协议和文件操作组成，并且可以包含筛选器列表。事件使用筛选器缩小 FPolicy 外部引擎必须发送通知的受监控事件的列表范围。事件还指定策略是否监控卷操作。

3. 创建FPolicy持久存储(可选)。

   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。

   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 9.15.1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。

4. 创建 FPolicy 策略。

   FPolicy 策略负责将需要监控的一组事件与相应的范围关联起来，以及必须将哪些受监控事件通知发送到指定的 FPolicy 服务器（如果未配置任何 FPolicy 服务器，则还必须发送到原生引擎）。该策略还定义是否允许 FPolicy 服务器对其接收通知的数据进行特权访问。如果 FPolicy 服务器需要访问数据，则需要进行特权访问。需要特权访问的典型使用情形包括文件阻止，配额管理和分层存储管理。您可以在此策略中指定此策略的配置是使用 FPolicy 服务器还是使用内部 "`原生` FPolicy 服务器。

策略指定是否必须进行筛选。如果必须进行筛选，并且所有 FPolicy 服务器均已关闭，或者在定义的超时期限内未从 FPolicy 服务器收到任何响应，则会拒绝文件访问。

策略的边界为 SVM 。一个策略不能应用于多个 SVM 。但是，一个特定 SVM 可以具有多个 FPolicy 策略，每个策略的范围，事件和外部服务器配置组合相同或不同。

5. 配置策略范围。

   FPolicy 范围用于确定该策略对哪些卷，共享或导出策略执行操作或排除在监控范围之外。范围还决定了应在 FPolicy 监控中包括或排除哪些文件扩展名。

   排除列表优先于包括列表。

6. 启用 FPolicy 策略。

   启用此策略后，控制通道以及（可选）有权限的数据通道将连接起来。SVM 参与的节点上的 FPolicy 进程开始监控文件和文件夹访问，对于符合已配置标准的事件，会向 FPolicy 服务器（如果未配置任何 FPolicy 服务器，则向原生引擎发送通知）。

如果此策略使用原生文件阻止，则不会配置外部引擎或将其与此策略关联。

规划 FPolicy 外部引擎配置

规划 ONTAP FPolicy 外部引擎配置

在配置FPolicy外部引擎之前、您必须了解创建外部引擎的含义以及可用的配置参数。此信息可帮助您确定要为每个参数设置的值。

创建 FPolicy 外部引擎时定义的信息

外部引擎配置用于定义FPolicy建立和管理与外部FPolicy服务器的连接所需的信息、其中包括：

- SVM name
- 引擎名称
- 主和二级 FPolicy 服务器的 IP 地址以及在连接到 FPolicy 服务器时要使用的 TCP 端口号
- 引擎类型是异步还是同步
- 引擎格式是否为 `xml` 或 `protobuf`

  从ONTAP 9.15.1开始、您可以使用 `protobuf` 引擎格式。设置为时 `protobuf`、通知消息使用Google Protobuf以二进制格式进行编码。将引擎格式设置为之前 `protobuf`下，请确保`FPolicy`服务器也支持 `protobuf` 反序列化。

  由于从ONTAP 9.15.1开始支持原始缓冲区格式、因此在还原到早期版本的ONTAP之前、您必须考虑外部引擎格式。如果还原到ONTAP 9.15.1之前的版本、请与FPolicy合作伙伴合作执行以下操作之一：

  - 从更改每个引擎格式 `protobuf` to `xml`
  - 删除引擎格式为的引擎 `protobuf`

- 如何对节点与 FPolicy 服务器之间的连接进行身份验证

  如果您选择配置相互 SSL 身份验证，则还必须配置提供 SSL 证书信息的参数。

- 如何使用各种高级权限设置管理连接

  其中包括用于定义超时值，重试值，保活值，最大请求值，已发送和接收缓冲区大小值以及会话超时值等内容的参数。

。 `vserver fpolicy policy external-engine create` 命令用于创建FPolicy外部引擎。

什么是基本外部引擎参数

您可以使用下表中的基本 FPolicy 配置参数来帮助您规划配置：

信息类型	选项
SVM 指定要与此外部引擎关联的 SVM 名称。 每个 FPolicy 配置都在一个 SVM 中定义。为创建 FPolicy 策略配置而组合在一起的外部引擎，策略事件，策略范围和策略都必须与同一 SVM 相关联。	`-vserver vserver_name`
引擎名称 _ 指定要分配给外部引擎配置的名称。您必须在稍后创建 FPolicy 策略时指定外部引擎名称。这会将外部引擎与策略相关联。 此名称最长可为 256 个字符。 如果在 MetroCluster 或 SVM 灾难恢复配置中配置外部引擎名称，则此名称的长度应最多为 200 个字符。 此名称可以包含以下 ASCII 范围字符的任意组合： • `a` 到 `z` • `A` 到 `Z` • `0` 到 `9` • “_”、“-”, and "`.`Ω"	`-engine-name engine_name`

_ 主 FPolicy 服务器 _ 指定节点针对给定 FPolicy 策略向其发送通知的主 FPolicy 服务器。此值以逗号分隔的 IP 地址列表形式指定。 如果指定了多个主服务器 IP 地址，则 SVM 参与的每个节点都会在启用此策略时与每个指定的主 FPolicy 服务器创建一个控制连接。如果配置了多个主 FPolicy 服务器，则会以轮循方式向 FPolicy 服务器发送通知。 如果在 MetroCluster 或 SVM 灾难恢复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。	`-primary-servers IP_address、`
端口号 _ 指定 FPolicy 服务的端口号。	`-port integer`
二级 FPolicy 服务器 _ 指定要将给定 FPolicy 策略的文件访问事件发送到的二级 FPolicy 服务器。此值以逗号分隔的 IP 地址列表形式指定。 只有在无法访问主服务器时，才会使用二级服务器。启用策略后，系统会建立与二级服务器的连接，但只有在无法访问任何主服务器时，才会向二级服务器发送通知。如果配置了多个二级服务器，则会以轮循方式向 FPolicy 服务器发送通知。	`-secondary-servers IP_address、`
外部引擎类型 _ 指定外部引擎是在同步模式还是异步模式下运行。默认情况下， FPolicy 在同步模式下运行。 设置为时 `synchronous`，文件请求处理会向FPolicy服务器发送通知，但只有在收到FPolicy服务器的响应后才会继续。此时，请求流将继续，或者处理将导致拒绝，具体取决于 FPolicy 服务器的响应是否允许所请求的操作。 设置为时 `asynchronous`，文件请求处理会向FPolicy服务器发送通知，然后继续。	`-extern-engine-type external_engine_type` 此参数的值可以是以下值之一： • `synchronous` • `asynchronous`
外部引擎格式_ 指定外部引擎格式是xml还是protobuf。 从ONTAP 9.15.1开始、您可以使用protobuf引擎格式。设置为protobuf时、通知消息将使用Google Protobuf以二进制格式进行编码。在将引擎格式设置为protobuf之前、请确保FPolicy服务器也支持protobuf反序列化。	`- extern-engine-format {protobuf 或 xml}`

用于与 FPolicy server_ 通信的 _ssl 选项 指定用于与 FPolicy 服务器通信的 SSL 选项。这是必需的参数。您可以根据以下信息选择一个选项： • 设置为时 `no-auth`，则不进行身份验证。 通信链路通过 TCP 建立。 • 设置为时 `server-auth`，SVM使用SSL服务器身份验证对FPolicy服务器进行身份验证。 • 设置为时 `mutual-auth`，SVM和FPolicy服务器之间会进行相互身份验证；SVM会对FPolicy服务器进行身份验证，FPolicy服务器会对SVM进行身份验证。 如果选择配置相互SSL身份验证、则还必须配置 `-certificate -common-name`， `-certificate-serial`，和 `-certifcate-ca` parameters	`-ssl-option` {`no-auth`
`server-auth`	`mutual-auth`}
证书 FQDN 或自定义公用名 _ 指定在 SVM 和 FPolicy 服务器之间配置 SSL 身份验证时使用的证书名称。您可以将证书名称指定为 FQDN 或自定义公用名。 如果指定 `mutual-auth` 。 `-ssl-option` 参数、则必须为指定一个值 `-certificate-common-name` 参数。	`-certificate-common -name` `text`
证书序列号 _ 指定在 SVM 和 FPolicy 服务器之间配置了 SSL 身份验证时用于身份验证的证书的序列号。 如果指定 `mutual-auth` 。 `-ssl-option` 参数、则必须为指定一个值 `-certificate-serial` 参数。	`-certificate-serial` `text`
证书颁发机构 _ 指定在 SVM 和 FPolicy 服务器之间配置了 SSL 身份验证时用于身份验证的证书的 CA 名称。 如果指定 `mutual-auth` 。 `-ssl-option` 参数、则必须为指定一个值 `-certificate-ca` 参数。	`-certificate-ca` `text`

什么是高级外部引擎选项

在计划是否使用高级参数自定义配置时，您可以使用下表中的高级 FPolicy 配置参数。您可以使用以下参数修改集群节点和 FPolicy 服务器之间的通信行为：

信息类型	选项
取消请求时超时 _ 指定时间间隔(以小时为单位) (h)、分钟 (m)或秒 (s)、表示节点等待FPolicy服务器的响应。 如果超时间隔已过，则节点会向 FPolicy 服务器发送取消请求。然后，节点会将通知发送到备用 FPolicy 服务器。此超时有助于处理无响应的 FPolicy 服务器，从而提高 SMB/NFS 客户端响应速度。此外，在超时期限后取消请求有助于释放系统资源，因为通知请求会从已关闭 / 错误的 FPolicy 服务器移至备用 FPolicy 服务器。 此值的范围为 0 到 100。如果此值设置为 0，选项已禁用，并且取消请求消息不会发送到FPolicy服务器。默认值为 20s。	-reqs-cancel-timeout integer[h
m	s]
中止请求时超时 _ 以小时为单位指定超时 (h)、分钟 (m)或秒 (s)以使请求发生abording。 此值的范围为 0 到 200。	-reqs-abort-timeout ` `integer[h
m	s]
发送状态请求的间隔 _ 以小时为单位指定间隔 (h)、分钟 (m)或秒 (s)之后、状态请求将发送到FPolicy服务器。 此值的范围为 0 到 50。如果此值设置为 0，选项已禁用，并且状态请求消息不会发送到FPolicy服务器。默认值为 10s。	-status-req-interval integer[h
m	s]
FPolicy 服务器上的最大未处理请求数 _ 指定可在 FPolicy 服务器上排队的最大未处理请求数。 此值的范围为 1 到 10000。默认值为 500。	-max-server-reqs integer

断开无响应 FPolicy 服务器的超时 _ 指定时间间隔(以小时为单位) (h)、分钟 (m)或秒 (s)之后、与FPolicy服务器的连接将终止。 只有当 FPolicy 服务器的队列包含允许的最大请求且在超时期限内未收到响应时，此连接才会在超时期限后终止。允许的最大请求数为任一 50 (默认值)或指定的数字 max-server-reqs- 参数。 此值的范围为 1 到 100。默认值为 60s。	-server-progress -timeout integer[h
m	s]
向 FPolicy 服务器发送保活消息的 _Interval 指定时间间隔(以小时为单位) (h)、分钟 (m)或秒 (s)、在该位置、保活消息将发送到FPolicy服务器。 保持活动消息会检测半打开的连接。 此值的范围为 10 到 600。如果此值设置为 0，选项将被禁用，并阻止将保持活动消息发送到FPolicy服务器。默认值为 120s。	-keep-alive-interval- integer[h
m	s]
最大重新连接尝试次数 _ 指定在连接断开后 SVM 尝试重新连接到 FPolicy 服务器的最大次数。 此值的范围为 0 到 20。默认值为 5。	-max-connection-retries integer
接收缓冲区大小 _ 指定 FPolicy 服务器的已连接套接字的接收缓冲区大小。 默认值设置为 256 KB 。如果此值设置为 0 ，则接收缓冲区的大小将设置为系统定义的值。 例如，如果套接字的默认接收缓冲区大小为 65536 字节，则通过将可调值设置为 0 ，套接字缓冲区大小将设置为 65536 字节。您可以使用任何非默认值来设置接收缓冲区的大小（以字节为单位）。	-recv-buffer-size integer

发送缓冲区大小 _ 指定 FPolicy 服务器的已连接套接字的发送缓冲区大小。 默认值设置为 256 KB 。如果此值设置为 0 ，则发送缓冲区的大小将设置为系统定义的值。 例如，如果套接字的默认发送缓冲区大小设置为 65536 字节，则通过将可调值设置为 0 ，套接字缓冲区大小将设置为 65536 字节。您可以使用任何非默认值来设置发送缓冲区的大小（以字节为单位）。	`-send-buffer-size integer`
_Timeout ，用于在重新连接期间清除会话 ID 以小时为单位指定间隔 (`h`)、分钟 (`m`)或秒 (`s`)之后、新会话ID将在重新连接尝试期间发送到FPolicy服务器。 如果存储控制器与FPolicy服务器之间的连接终止、并在中重新建立连接 `-session-timeout` 间隔、旧会话ID将发送到FPolicy服务器、以便它可以发送对旧通知的响应。 默认值设置为10秒。	`-session-timeout [integerh][integerm][integer秒]`

有关配置 **ONTAP FPolicy** 外部引擎以使用 **SSL** 身份验证连接的其他信息

如果要将 FPolicy 外部引擎配置为在连接到 FPolicy 服务器时使用 SSL ，则需要了解一些追加信息。

SSL 服务器身份验证

如果选择为 SSL 服务器身份验证配置 FPolicy 外部引擎，则在创建外部引擎之前，必须安装对 FPolicy 服务器证书签名的证书颁发机构（ CA ）的公有证书。

相互身份验证

如果您将 FPolicy 外部引擎配置为在将 Storage Virtual Machine （ SVM ）数据 LIF 连接到外部 FPolicy 服务器时使用 SSL 相互身份验证，则在创建外部引擎之前， 您必须安装对 FPolicy 服务器证书签名的 CA 的公有证书以及公有证书和密钥文件，以便对 SVM 进行身份验证。当任何FPolicy策略都在使用已安装的证书时、请勿删除此证书。

如果在连接到外部 FPolicy 服务器时 FPolicy 使用该证书进行相互身份验证时删除了该证书，则无法重新启用使用该证书的已禁用 FPolicy 策略。在这种情况下，即使在 SVM 上创建并安装了具有相同设置的新证书，也无法重新启用 FPolicy 策略。

如果证书已删除，则需要安装新证书，创建使用新证书的新 FPolicy 外部引擎，并通过修改 FPolicy 策略将新外部引擎与要重新启用的 FPolicy 策略相关联。

安装 **SSL** 证书

用于签署FPolicy服务器证书的CA的公共证书是使用安装的 `security certificate install` 命令 `-type` 参数设置为 `client-ca`。使用安装SVM身份验证所需的专用密钥和公共证书 `security certificate`

install 命令 -type 参数设置为 server。

相关信息

- "安全证书安装"

ONTAP FPolicy 证书不会在具有非 ID 保留配置的 SVM 灾难恢复关系中复制

在连接到 FPolicy 服务器时用于 SSL 身份验证的安全证书不会复制到具有非 ID-preserve 配置的 SVM 灾难恢复目标。虽然会复制 SVM 上的 FPolicy 外部引擎配置，但不会复制安全证书。您必须在目标上手动安装安全证书。

在设置SVM灾难恢复关系时、您为选择的值 -identity-preserve 的选项 snapmirror create 命令用于确定复制到目标SVM中的配置详细信息。

如果您设置了 -identity-preserve 选项 true (ID保留)、则会复制所有FPolicy配置详细信息、包括安全证书信息。只有在将选项设置为时、才必须在目标上安装安全证书 false (不保留ID)。

相关信息

- "SnapMirror 创建"

具有 MetroCluster 和 SVM 灾难恢复配置的集群范围 ONTAP FPolicy 外部引擎的限制

您可以通过将集群 Storage Virtual Machine （ SVM ）分配给外部引擎来创建集群范围的 FPolicy 外部引擎。但是，在 MetroCluster 或 SVM 灾难恢复配置中创建集群范围的外部引擎时，在选择 SVM 用于与 FPolicy 服务器进行外部通信的身份验证方法时，存在某些限制。

创建外部 FPolicy 服务器时，您可以选择三种身份验证选项：无身份验证， SSL 服务器身份验证和 SSL 相互身份验证。尽管在将外部 FPolicy 服务器分配给数据 SVM 时选择身份验证选项没有任何限制，但在创建集群范围的 FPolicy 外部引擎时仍存在一些限制：

Configuration	是否允许?
MetroCluster 或 SVM 灾难恢复以及集群范围的 FPolicy 外部引擎，不进行身份验证（未配置 SSL ）	是的。
MetroCluster 或 SVM 灾难恢复以及具有 SSL 服务器或 SSL 相互身份验证的集群范围 FPolicy 外部引擎	否

- 如果存在具有 SSL 身份验证的集群范围的 FPolicy 外部引擎，而您要创建 MetroCluster 或 SVM 灾难恢复配置，则必须先修改此外部引擎以不使用身份验证或删除外部引擎，然后才能创建 MetroCluster 或 SVM 灾难恢复配置。
- 如果 MetroCluster 或 SVM 灾难恢复配置已存在，则 ONTAP 会阻止您使用 SSL 身份验证创建集群范围的 FPolicy 外部引擎。

完成 ONTAP FPolicy 外部引擎配置工作表

您可以使用此工作表记录 FPolicy 外部引擎配置过程中所需的值。如果需要参数值，您需

要先确定要对这些参数使用的值，然后再配置外部引擎。

基本外部引擎配置的信息

您应记录是否要在外部引擎配置中包括每个参数设置，然后记录要包括的参数的值。

信息类型	Required	包括	您的价值
Storage Virtual Machine （ SVM ）名称	是的。	是的。	
引擎名称	是的。	是的。	
主 FPolicy 服务器	是的。	是的。	
端口号	是的。	是的。	
二级 FPolicy 服务器	否		
外部引擎类型	否		
用于与外部 FPolicy 服务器通信的 SSL 选项	是的。	是的。	
证书 FQDN 或自定义公用名	否		
证书序列号	否		
证书颁发机构	否		

有关高级外部引擎参数的信息

要使用高级参数配置外部引擎，必须在高级权限模式下输入配置命令。

信息类型	Required	包括	您的价值
取消请求超时	否		
中止请求超时	否		
发送状态请求的间隔	否		
FPolicy 服务器上的最大未处理请求数	否		
断开无响应 FPolicy 服务器的连接超时	否		

向 FPolicy 服务器发送保活消息的间隔	否		
最大重新连接尝试次数	否		
接收缓冲区大小	否		
发送缓冲区大小	否		
重新连接期间清除会话 ID 超时	否		

规划 FPolicy 事件配置

了解ONTAP FPolicy事件配置

在配置 FPolicy 事件之前，您必须了解创建 FPolicy 事件的含义。您必须确定要监控事件的协议，要监控的事件以及要使用的事件筛选器。此信息有助于您规划要设置的值。

创建 FPolicy 事件的含义

创建 FPolicy 事件意味着定义 FPolicy 进程需要用于确定要监控的文件访问操作以及应将哪些受监控事件通知发送到外部 FPolicy 服务器的信息。FPolicy 事件配置定义了以下配置信息：

- Storage Virtual Machine （ SVM ）名称
- 事件名称
- 要监控的协议

  从ONTAP 9.15.1开始、FPolicy可以监控SMB、NFSv3、NFSv4以及NFSv4.1文件访问操作。

- 要监控的文件操作

  并非所有文件操作对每个协议都有效。

- 要配置的文件筛选器

  只有某些文件操作和筛选器组合有效。每个协议都有自己一组支持的组合。

- 是否监控卷挂载和卸载操作

> 其中三个参数具有相关性 (`-protocol`， `-file-operations`， `-filters`）。以下组合适用于这三个参数：
>
> - 您可以指定 `-protocol` 和 `-file-operations` parameters
> - 您可以指定所有三个参数。
> - 您不能指定任何参数。

FPolicy 事件配置包含的内容

您可以使用以下可用 FPolicy 事件配置参数列表来帮助您规划配置：

信息类型	选项
SVM 指定要与此 FPolicy 事件关联的 SVM 名称。 每个 FPolicy 配置都在一个 SVM 中定义。为创建 FPolicy 策略配置而组合在一起的外部引擎，策略事件，策略范围和策略都必须与同一 SVM 相关联。	`-vserver vserver_name`
事件名称 _ 指定要分配给 FPolicy 事件的名称。创建 FPolicy 策略时，您可以使用事件名称将 FPolicy 事件与策略相关联。 此名称最长可为 256 个字符。 ⓘ 如果在 MetroCluster 或 SVM 灾难恢复配置中配置事件，则此名称的长度应最多为 200 个字符。 此名称可以包含以下 ASCII 范围字符的任意组合： • `a` 到 `z` • `A` 到 `Z` • `0` 到 `9` • " _ "、“-”, and "`.`Ω"	`-event-name event_name`
_ 协议 _ 指定要为 FPolicy 事件配置的协议。的列表 `-protocol` 可以包含以下值之一： • `cifs` • `nfsv3` • `nfsv4` ⓘ 如果指定 `-protocol`则必须在中指定有效值 `-file-operations` 参数。协议版本发生变化时，有效值可能会发生变化。 ⓘ 从ONTAP 9.15.1开始、您可以通过NFSv4捕获NFSv4.0和NFSv4.1事件。	`-protocol protocol`

File operations 指定 FPolicy 事件的文件操作列表。 此事件使用中指定的协议从所有客户端请求中检查此列表中指定的操作 `-protocol` 参数。您可以使用逗号分隔列表列出一个或多个文件操作。的列表 `-file-operations` 可以包含以下一个或多个值： • `close` 用于文件关闭操作 • `create` 用于文件创建操作 • `create-dir` 目录创建操作 • `delete` 用于文件删除操作 • `delete_dir` 目录删除操作 • `getattr` 获取属性操作 • `link` 用于链路操作 • `lookup` 查找操作 • `open` 用于文件打开操作 • `read` 用于文件读取操作 • `write` 用于文件写入操作 • `rename` 用于文件重命名操作 • `rename_dir` 目录重命名操作 • `setattr` 用于设置属性操作 • `symlink` 符号链接操作 如果指定 `-file-operations`，则必须在中指定有效的协议 `-protocol` 参数。	`-file-operations file_operations、`

Filters 指定指定协议的给定文件操作的筛选器列表。中的值 `-filters` 参数用于筛选客户端请求。此列表可以包括以下一项或多项： 如果指定 `-filters` 参数、则还必须为指定有效值 `-file-operations` 和 `-protocol` parameters • `monitor-ads` 用于筛选客户端对备用数据流的请求的选项。 • `close-with-modification` 用于筛选客户端请求以关闭并修改的选项。 • `close-without-modification` 用于筛选客户端请求以进行关闭而不进行修改的选项。 • `first-read` 用于筛选客户端请求以进行首次读取的选项。 • `first-write` 用于筛选客户端请求以进行首次写入的选项。 • `offline-bit` 用于筛选脱机位集的客户端请求的选项。 设置此筛选器会使 FPolicy 服务器仅在访问脱机文件时收到通知。 • `open-with-delete-intent` 用于筛选客户端请求的选项、以用于具有删除意图的OPEN。 设置此筛选器后，只有在尝试打开要删除的文件时， FPolicy 服务器才会收到通知。当时、文件系统会使用此选项 `FILE_DELETE_ON_CLOSE` 已指定标志。 • `open-with-write-intent` 用于筛选具有写入意图的OPEN客户端请求的选项。 设置此筛选器后，只有在尝试打开文件并在其中写入内容时， FPolicy 服务器才会收到通知。 • `write-with-size-change` 用于筛选客户端写入请求并更改大小的选项。 • `setattr-with-owner-change` 用于筛选客户端SETATTR更改文件或目录所有者的请求的选项。 • `setattr-with-group-change` 用于筛选客户端SETATTR更改文件或目录组的请求的选项。 • `setattr-with-sacl-change` 用于筛选客户端SETATTR更改文件或目录上的SACL请求的选项。 此筛选器仅适用于SMB和NFSv4协议。 • `setattr-with-dacl-change` 用于筛选客户端SETATTR请求以更改文件或目录上的DACL的选项。 此筛选器仅适用于SMB和NFSv4协议。 `setattr-with-modify-time-change` 用于筛选客户端SETATTR请求以更改文件或目录的修改时间的选项。 `setattr-with-access-time-change` 用于筛选客户端setattr请求以	`-filters filter，...`

是否需要执行卷操作 _ 指定卷挂载和卸载操作是否需要监控。默认值为 `false`。	`-volume-operation {true`

`false}`
 	
`-filters filter, ...`
	*FPolicy*访问被拒绝通知
	
	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。如果文件操作因缺少权限而失败、则会生成通知、其中包括：
	
	• 由于NTFS权限而失败。
	• 由于Unix模式位而导致失败。
	• 由于NFSv4 ACL而导致失败。

`-monitor-fileop-failure {true`	`false}`

ONTAP FPolicy 监控 SMB 支持的文件操作和过滤器组合

在配置 FPolicy 事件时，您需要注意的是，监控 SMB 文件访问操作仅支持特定的文件操作和筛选器组合。

下表列出了用于监控 SMB 文件访问事件的 FPolicy 支持的文件操作和筛选器组合：

支持的文件操作	支持的筛选器
关闭	监控器广告，脱机位，修改后接近，修改后关闭，读取后关闭， 排除目录
创建	监控器广告，脱机位
create_dir	目前，此文件操作不支持任何筛选器。
删除	监控器广告，脱机位
delete_dir	目前，此文件操作不支持任何筛选器。
getattr	offline-bit ， exclude-dir
打开	monitor-ad ， offline-bit ， open-wan-delete-intent ， open-write-intent ， exclude-dir

读取	监控器广告，脱机位，首次读取
写入	monitor-ad ， offline-bit ， first-write ， write-write-wing-write-size-change
重命名	监控器广告，脱机位
rename_dir	目前，此文件操作不支持任何筛选器。
SETATTR	monitor-ad ， offline-bit ， setattr_and_owner_change ， setattr_and_group_change ， setattr_and_mode_change ， setattr_for_sacl_change ， setattr_for_dacl_change ， setattr_for_modify_time_change ， setattr_for_access_time_change ， setattr_for_creation_time_change ， setattr_and_size_change ， setattr_and_allocation_size_change ， exclude_directory

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。下表列出了在对SMB文件访问事件进行FPolicy监控时支持的拒绝访问文件操作和筛选器组合：

支持拒绝访问文件操作	支持的筛选器
打开	不适用

ONTAP FPolicy 为 NFSv3 监控的支持的文件操作和过滤器组合

配置FPolicy事件时、需要注意、仅支持使用特定的文件操作和筛选器组合来监控NFSv3文件访问操作。

下表列出了对NFSv3文件访问事件执行FPolicy监控时支持的文件操作和筛选器组合：

支持的文件操作	支持的筛选器
创建	脱机位
create_dir	目前，此文件操作不支持任何筛选器。
删除	脱机位
delete_dir	目前，此文件操作不支持任何筛选器。
链接。	脱机位
查找	offline-bit ， exclude-dir
读取	脱机位，首次读取

写入	脱机位，首次写入，写入时更改大小
重命名	脱机位
rename_dir	目前，此文件操作不支持任何筛选器。
SETATTR	脱机位， setattr_and_owner_change ， setattr_and_group_change ， setattr_and_mode_change ， setattr_and_modify_time_change ， setattr_and_access_time_change ， setattr_and_size_change ， exclude_directory
符号链接	脱机位

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。下表列出了对NFSv3文件访问事件进行FPolicy监控时支持的拒绝访问文件操作和筛选器组合：

支持拒绝访问文件操作	支持的筛选器
访问	不适用
创建	不适用
create_dir	不适用
删除	不适用
delete_dir	不适用
链接。	不适用
读取	不适用
重命名	不适用
rename_dir	不适用
SETATTR	不适用
写入	不适用

ONTAP FPolicy 为 NFSv4 监控的支持的文件操作和过滤器组合

在配置 FPolicy 事件时，您需要注意，在监控 NFSv4 文件访问操作时，仅支持特定的文件操作和筛选器组合。

从ONTAP 9.15.1开始、FPolicy支持NFSv4.1协议。

下表列出了对NFSv4或NFSv4.1文件访问事件执行FPolicy监控时支持的文件操作和筛选器组合：

支持的文件操作	支持的筛选器
关闭	脱机位，排除目录
创建	脱机位
create_dir	目前，此文件操作不支持任何筛选器。
删除	脱机位
delete_dir	目前，此文件操作不支持任何筛选器。
getattr	脱机位，排除目录
链接。	脱机位
查找	脱机位，排除目录
打开	脱机位，排除目录
读取	脱机位，首次读取
写入	脱机位，首次写入，写入时更改大小
重命名	脱机位
rename_dir	目前，此文件操作不支持任何筛选器。
SETATTR	脱机位， setattr_and_owner_change ， setattr_and_group_change ， setattr_and_mode_change ， setattr_and_sacl_change ， setattr_and_dacl_change ， setattr_and_modify_time_change ， setattr_and_access_time_change ， setattr_and_size_change ， exclude_directory
符号链接	脱机位

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。下表列出了对NFSv4或NFSv4.1文件访问事件执行FPolicy监控时支持的拒绝访问文件操作和筛选器组合：

支持拒绝访问文件操作	支持的筛选器

访问	不适用
创建	不适用
create_dir	不适用
删除	不适用
delete_dir	不适用
链接。	不适用
打开	不适用
读取	不适用
重命名	不适用
rename_dir	不适用
SETATTR	不适用
写入	不适用

完成 **ONTAP FPolicy** 事件配置工作表

您可以使用此工作表记录 FPolicy 事件配置过程中所需的值。如果需要参数值，则需要先确定要对这些参数使用的值，然后再配置 FPolicy 事件。

您应记录是否要在 FPolicy 事件配置中包括每个参数设置，然后记录要包括的参数的值。

信息类型	Required	包括	您的价值
Storage Virtual Machine （ SVM ）名称	是的。	是的。	
事件名称	是的。	是的。	
协议	否		
文件操作	否		
筛选器	否		

卷操作	否		
拒绝访问事件+ (从ONTAP 9.13开始提供支持)	否		

规划 FPolicy 策略配置

了解 ONTAP FPolicy 策略配置

在配置 FPolicy 策略之前，您必须了解创建策略时需要哪些参数，以及为什么要配置某些可选参数。此信息可帮助您确定要为每个参数设置的值。

创建 FPolicy 策略时，请将此策略与以下项相关联：

- Storage Virtual Machine （ SVM ）
- 一个或多个 FPolicy 事件
- FPolicy 外部引擎

您还可以配置多个可选策略设置。

FPolicy 策略配置包含哪些内容

您可以使用以下可用的 FPolicy 必需策略和可选参数列表来帮助您规划配置：

信息类型	选项	Required	Default
_SVM 名称 _ 指定要在其中创建 FPolicy 策略的 SVM 的名称。	`-vserver vserver_name`	是的。	无

策略名称 _ 指定 FPolicy 策略的名称。 此名称最长可为 256 个字符。 如果在 MetroCluster 或 SVM 灾难恢复配置中配置策略，则此名称的长度应最多为 200 个字符。 此名称可以包含以下 ASCII 范围字符的任意组合： • a 到 z • A 到 Z • 0 到 9 • “_”、“-”, and "`.`Ω"	-policy-name policy_name	是的。	无
事件名称 _ 指定要与 FPolicy 策略关联的事件的逗号分隔列表。 • 您可以将多个事件关联到一个策略。 • 事件是特定于协议的。 • 您可以使用一个策略来监控多个协议的文件访问事件，方法是为要策略监控的每个协议创建一个事件，然后将事件与策略关联。 • 事件必须已存在。	-events event_name，...	是的。	无
持久性存储 从ONTAP 9.14.1开始、此参数用于指定永久性存储、以捕获SVM中异步非强制策略的文件访问事件。	-persistent -store persistent_store_name	否	无

外部引擎名称 _ 指定要与 FPolicy 策略关联的外部引擎的名称。 • 外部引擎包含节点向 FPolicy 服务器发送通知所需的信息。 • 您可以将 FPolicy 配置为使用 ONTAP 原生外部引擎进行简单文件阻止，或者使用配置为使用外部 FPolicy 服务器（FPolicy 服务器）的外部引擎进行更复杂的文件阻止和文件管理。 • 如果要使用本机外部引擎、则不能为此参数指定值、也可以指定 `native` 作为值。 • 如果要使用 FPolicy 服务器，外部引擎的配置必须已存在。	`-engine engine_name`	是（除非策略使用内部 ONTAP 原生引擎）	`native`
Is mandatory screening required 指定是否需要强制文件访问筛选。 • 强制筛选设置用于确定在所有主服务器和二级服务器均已关闭或在给定超时期限内未从 FPolicy 服务器收到响应时对文件访问事件采取的操作。 • 设置为时 `true`，文件访问事件被拒绝。 • 设置为时 `false`，则允许文件访问事件。	`-is-mandatory {true`	`false}`	否

true	*allow privileged access* 指定是否希望 FPolicy 服务器通过使用有权限的数据连接对受监控的文件和文件夹具有访问权限。 如果已配置，则 FPolicy 服务器可以使用特权数据连接从 SVM 的根目录访问包含受监控数据的文件。 要进行有权限的数据访问、必须在集群上获得SMB的许可、并且必须将用于连接到FPolicy服务器的所有数据SIFs配置为具有 `cifs` 作为允许的协议之一。 如果要将策略配置为允许特权访问，则还必须为希望 FPolicy 服务器用于特权访问的帐户指定用户名。	`-allow -privileged -access {yes`	`no}`
否（除非启用直通读取）	`no`	特权用户名 _ 指定 FPolicy 服务器用于特权数据访问的帐户的用户名。 • 此参数的值应采用 `domain\username` 格式。 • 条件 `-allow -privileged -access` 设置为 `no`，则会忽略为此参数设置的任何值。	`-privileged -user-name user_name`

否（除非启用了特权访问）	无	*allow passthrough-read* 指定 FPolicy 服务器是否可以为已由 FPolicy 服务器归档到二级存储（脱机文件）的文件提供直通读取服务： • 直通读取是一种在不将数据还原到主存储的情况下读取脱机文件数据的方法。 直通读取可减少响应延迟，因为在响应读取请求之前，无需将文件重新调用回主存储。此外，直通读取还可以通过消除仅为满足读取请求而重新调用的文件占用主存储空间的需求来优化存储效率。 • 启用后，FPolicy 服务器将通过专为直通读取打开的单独有权限的数据通道为文件提供数据。 • 如果要配置直通读取，则还必须将策略配置为允许特权访问。	`-is-passthrough-read-enabled {true`

如果 **FPolicy** 策略使用本机引擎，则需要 **ONTAP FPolicy** 范围配置

如果您将 FPolicy 策略配置为使用原生引擎，则需要明确说明如何定义为该策略配置的 FPolicy 范围。

FPolicy 范围定义了应用 FPolicy 策略的边界，例如 FPolicy 适用场景是否指定了卷或共享。有许多参数进一步限制了 FPolicy 策略的适用范围。其中一个参数、 `-is-file-extension-check-on-directories-enabled`，指定是否检查目录上的文件扩展名。默认值为 `false`，表示不检查目录上的文件扩展名。

在共享或卷以及上启用使用本机引擎的FPolicy策略时 `-is-file-extension-check-on-directories-enabled` 参数设置为 `false` 对于策略范围、目录访问将被拒绝。使用此配置时，由于不会检查文件扩展名中是否存在目录，因此，如果任何目录操作属于此策略的范围，则会拒绝此操作。

要确保在使用本机引擎时成功访问目录、您必须设置 `-is-file-extension-check-on-directories-enabled parameter` to `true` 创建范围时。

将此参数设置为 `true`，将对目录操作进行扩展检查，并根据FPolicy范围配置中包含或排除的扩展来决定是允许还是拒绝访问。

完成 ONTAP FPolicy 策略工作表

您可以使用此工作表记录 FPolicy 策略配置过程中所需的值。您应记录是否要在 FPolicy 策略配置中包括每个参数设置，然后记录要包括的参数的值。

信息类型	包括	您的价值
Storage Virtual Machine （ SVM ）名称	是的。	
Policy name	是的。	
事件名称	是的。	
永久性存储		
外部引擎名称		
是否需要强制筛查?		
允许特权访问		
有权限的用户名		
是否已启用直通读取?		

规划 FPolicy 范围配置

了解 ONTAP FPolicy 范围配置

在配置 FPolicy 范围之前，您必须了解创建范围的含义。您必须了解范围配置的内容。您还需要了解优先级范围规则的含义。此信息可帮助您规划要设置的值。

创建 FPolicy 范围的含义

创建 FPolicy 范围意味着定义适用 FPolicy 策略的边界。Storage Virtual Machine （ SVM ）是基本边界。在为 FPolicy 策略创建范围时，必须定义要应用此范围的 FPolicy 策略，并且必须指定要应用此范围的 SVM 。

有许多参数进一步限制了指定 SVM 中的范围。您可以通过指定要包含在范围中的内容或指定要从范围中排除的内容来限制范围。将范围应用于已启用的策略后，策略事件检查将应用于此命令定义的范围。

如果在 "`include` " 选项中找到匹配项，则会为文件访问事件生成通知。如果在 "`exclude` " 选项中找到匹配项，则不会为文件访问事件生成通知。

FPolicy 范围配置定义了以下配置信息：

- SVM name
- Policy name
- 要包括或排除受监控内容的共享
- 要包括或排除受监控内容的导出策略
- 要包括或排除受监控内容的卷
- 要在受监控的内容中包含或排除的文件扩展名
- 是否对目录对象执行文件扩展名检查

> 有关集群 FPolicy 策略的范围，需要特别注意一些事项。集群 FPolicy 策略是集群管理员为管理 SVM 创建的策略。如果集群管理员还为该集群 FPolicy 策略创建了范围，则 SVM 管理员不能为同一策略创建范围。但是，如果集群管理员未为集群 FPolicy 策略创建范围，则任何 SVM 管理员都可以为该集群策略创建范围。如果 SVM 管理员为该集群 FPolicy 策略创建了范围，则集群管理员随后无法为同一集群策略创建集群范围。这是因为集群管理员不能覆盖同一集群策略的范围。

什么是优先级范围规则

以下优先级规则适用于范围配置：

- 当共享包含在中时 `-shares-to-include` 参数、共享的父卷包含在中 `-volumes-to-exclude` 参数、`-volumes-to-exclude` 优先于 `-shares-to-include`。
- 导出策略包含在中时 `-export-policies-to-include` 参数和导出策略的父卷包含在中 `-volumes-to-exclude` 参数、 `-volumes-to-exclude` 优先于 `-export-policies-to-include`。
- 管理员可以同时指定这两者 `-file-extensions-to-include` 和 `-file-extensions-to-exclude` 列表。

  。 `-file-extensions-to-exclude` 参数已在之前检查 `-file-extensions-to-include` 已检查参数。

FPolicy 范围配置包含的内容

您可以使用以下可用 FPolicy 范围配置参数列表来帮助您规划配置：

> 在配置要在范围中包括或排除的共享、导出策略、卷和文件扩展名时、include和exclude参数可以包括元字符、例如"`"?`" and “*”。 不支持使用正则表达式。

信息类型	选项

SVM 指定要创建 FPolicy 范围的 SVM 名称。 每个 FPolicy 配置都在一个 SVM 中定义。为创建 FPolicy 策略配置而组合在一起的外部引擎，策略事件，策略范围和策略都必须与同一 SVM 相关联。	`-vserver vserver_name`
策略名称 _ 指定要将范围附加到的 FPolicy 策略的名称。FPolicy 策略必须已存在。	`-policy-name policy_name`
要包含的共享 _ 指定要监控应用范围的 FPolicy 策略的共享列表，以逗号分隔。	`-shares-to-include share_name，...`
要排除的共享 _ 指定要从对应用了范围的 FPolicy 策略的监控中排除的共享的逗号分隔列表。	`-shares-to-exclude share_name，...`
要包含的卷 _ 指定要监控的卷列表，以确定应用了此范围的 FPolicy 策略。	`-volumes-to-include volume_name，...`
要排除的卷 _ 指定要从应用范围的 FPolicy 策略的监控中排除的卷的逗号分隔列表。	`-volumes-to-exclude volume_name，...`
导出要包含的策略 _ 指定一个以逗号分隔的导出策略列表，用于监控应用此范围的 FPolicy 策略。	`-export-policies-to -include export_policy_name，...`
导出要排除的策略 _ 指定要从对应用范围的 FPolicy 策略的监控中排除的导出策略的逗号分隔列表。	`-export-policies-to -exclude export_policy_name，...`
要包含的文件扩展名 _ 指定要监控应用范围的 FPolicy 策略的文件扩展名的逗号分隔列表。	`-file-extensions-to -include file_extensions，...`
要排除的文件扩展名 _ 指定要从对应用范围的 FPolicy 策略的监控中排除的文件扩展名的逗号分隔列表。	`-file-extensions-to -exclude file_extensions，...`

目录上的文件扩展名检查是否已启用？ _ 指定文件扩展名检查是否也应用于目录对象。如果此参数设置为 `true`，目录对象将接受与常规文件相同的扩展名检查。如果此参数设置为 `false`，目录名称与扩展名不匹配，即使目录的名称扩展名不匹配，也会为其发送通知。 如果将范围分配到的FPolicy策略配置为使用本机引擎、则必须将此参数设置为 `true`。	`-is-file-extension -check-on-directories -enabled {true`我们可以为您提供 `false`

完成 ONTAP FPolicy 范围工作表

您可以使用此工作表记录在 FPolicy 范围配置过程中所需的值。如果需要参数值，则需要先确定要对这些参数使用的值，然后再配置 FPolicy 范围。

您应记录是否要在 FPolicy 范围配置中包括每个参数设置，然后记录要包括的参数的值。

信息类型	Required	包括	您的价值
Storage Virtual Machine （ SVM ）名称	是的。	是的。	
Policy name	是的。	是的。	
要包含的共享	否		
要排除的共享	否		
要包含的卷	否		
要排除的卷	否		
要包括的导出策略	否		
要排除的导出策略	否		
要包括的文件扩展名	否		
要排除的文件扩展名	否		
是否已启用目录文件扩展名检查?	否		