



使用 FPolicy 在 SVM 上监控和管理文件

ONTAP 9

NetApp
January 09, 2026

目录

使用 FPolicy 在 SVM 上监控和管理文件	1
了解 FPolicy	1
了解ONTAP FPolicy 解决方案	1
ONTAP FPolicy 同步和异步通知	1
ONTAP FPolicy 持久存储	2
ONTAP FPolicy 配置类型	2
ONTAP FPolicy 实施中的集群组件角色	3
ONTAP FPolicy 如何与外部 FPolicy 服务器配合使用	4
节点到外部 ONTAP FPolicy 服务器通信过程	5
了解跨 SVM 命名空间的 ONTAP FPolicy 服务	7
ONTAP FPolicy 直通读取如何增强分层存储管理的可用性	7
规划 FPolicy 配置	8
配置 ONTAP FPolicy 的要求、注意事项和最佳实践	8
设置 ONTAP FPolicy 配置	13
规划 FPolicy 外部引擎配置	14
规划 FPolicy 事件配置	23
规划 FPolicy 策略配置	33
规划 FPolicy 范围配置	38
创建 FPolicy 配置	41
创建 ONTAP FPolicy 外部引擎	42
创建 ONTAP FPolicy 事件	43
创建 ONTAP FPolicy 持久存储	44
创建 ONTAP FPolicy 策略	46
创建 ONTAP FPolicy 范围	47
启用 ONTAP FPolicy 策略	48
管理 FPolicy 配置	49
修改 FPolicy 配置	49
显示有关 FPolicy 配置的信息	50
管理 FPolicy 服务器连接	53

使用 FPolicy 在 SVM 上监控和管理文件

了解FPolicy

了解ONTAP FPolicy 解决方案

FPolicy是一个文件访问通知框架、用于通过合作伙伴解决方案监控和管理Storage Virtual Machine (SVM)上的文件访问事件。合作伙伴解决方案可帮助您应对各种用例、例如数据监管与合规性、勒索软件保护和数据移动性。

合作伙伴解决方案包括NetApp支持的第三方解决方案和NetApp产品工作负载安全性和云数据感知。

FPolicy 解决方案分为两部分。ONTAP FPolicy框架可管理集群上的活动、并向合作伙伴应用程序(也称为外部FPolicy服务器)发送通知。外部FPolicy服务器处理ONTAP FPolicy发送的通知、以满足客户使用情形的要求。

ONTAP 框架可创建和维护 FPolicy 配置，监控文件事件并向外部 FPolicy 服务器发送通知。ONTAP FPolicy 提供的基础架构允许外部 FPolicy 服务器与 Storage Virtual Machine (SVM) 节点之间进行通信。

当由于客户端访问而发生某些文件系统事件时，FPolicy 框架会连接到外部 FPolicy 服务器，并向 FPolicy 服务器发送有关这些事件的通知。外部 FPolicy 服务器会处理通知并将响应发送回节点。由于通知处理而发生的情况取决于应用程序以及节点与外部服务器之间的通信是异步还是同步。

ONTAP FPolicy 同步和异步通知

FPolicy 会通过 FPolicy 接口向外部 FPolicy 服务器发送通知。通知以同步或异步模式发送。通知模式可确定 ONTAP 在向 FPolicy 服务器发送通知后执行的操作。

- * 异步通知 *

使用异步通知时，节点不会等待 FPolicy 服务器的响应，从而提高系统的整体吞吐量。此类通知适用于 FPolicy 服务器不要求在评估通知后执行任何操作的应用程序。例如，当 Storage Virtual Machine (SVM) 管理员希望监控和审核文件访问活动时，会使用异步通知。

如果在异步模式下运行的 FPolicy 服务器发生网络中断，则在中断期间生成的 FPolicy 通知将存储在存储节点上。当 FPolicy 服务器恢复联机时，它会收到存储的通知警报，并可从存储节点提取这些通知。在中断期间可以存储通知的时间长度可配置为长达 10 分钟。

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。

- * 同步通知 *

如果配置为在同步模式下运行，则 FPolicy 服务器必须确认每个通知，然后才能继续执行客户端操作。如果根据通知评估结果需要执行操作，则会使用此类型的通知。例如，当 SVM 管理员希望根据外部 FPolicy 服务器上指定的标准允许或拒绝请求时，将使用同步通知。

同步和异步应用程序

FPolicy 应用程序有许多可能的用途，包括异步和同步应用程序。

异步应用程序是指外部 FPolicy 服务器不会更改对文件或目录的访问权限或修改 Storage Virtual Machine (SVM) 上的数据的应用程序。例如：

- 文件访问和审核日志记录
- 存储资源管理

同步应用程序是指外部 FPolicy 服务器更改数据访问或修改数据的应用程序。例如：

- 配额管理
- 文件访问阻止
- 文件归档和分层存储管理
- 加密和解密服务
- 数据压缩和解压缩服务

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、您可以设置FPolicy永久性存储、以捕获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。

此功能仅在FPolicy外部模式下可用。您使用的合作伙伴应用程序需要支持此功能。您应与合作伙伴合作、确保此FPolicy配置受支持。

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、并使用永久性存储最佳实践配置卷。

有关持久性存储最佳实践的详细信息、请参见 "[配置 FPolicy 的要求，注意事项和最佳实践](#)"。

有关添加永久性存储的信息、请参见 "[创建持久性存储](#)"。

ONTAP FPolicy 配置类型

有两种基本的 FPolicy 配置类型。一种配置使用外部 FPolicy 服务器处理通知并对通知采取措施。另一种配置不使用外部 FPolicy 服务器，而是使用 ONTAP 内部原生 FPolicy 服务器根据扩展来简单地阻止文件。

- * 外部 FPolicy 服务器配置 *

此通知将发送到 FPolicy 服务器，该服务器会筛选请求并应用规则来确定节点是否应允许所请求的文件操作。对于同步策略， FPolicy 服务器会向节点发送响应，以允许或阻止请求的文件操作。

- * 原生 FPolicy 服务器配置 *

通知将在内部进行筛选。根据在 FPolicy 范围中配置的文件扩展名设置，允许或拒绝此请求。

注：不会记录被拒绝的文件扩展名请求。

何时创建原生 FPolicy 配置

原生 FPolicy 配置使用 ONTAP 内部 FPolicy 引擎根据文件扩展名监控和阻止文件操作。此解决方案不需要外部 FPolicy 服务器（ FPolicy 服务器）。如果只需使用此简单解决方案，则可以使用原生文件阻止配置。

通过原生文件阻止，您可以监控与配置的操作和筛选事件匹配的任何文件操作，然后拒绝访问具有特定扩展名的文件。这是默认配置。

此配置提供了一种仅根据文件扩展名阻止文件访问的方法。例如、阻止包含的文件 mp3 扩展名、则可以配置一个策略、以便为具有目标文件扩展名的某些操作提供通知 mp3。此策略配置为 deny mp3 生成通知的操作的文件请求。

以下适用场景原生 FPolicy 配置：

- 原生文件阻止也支持基于 FPolicy 服务器的文件筛选所支持的同一组筛选器和协议。
- 可以同时配置原生文件阻止和基于 FPolicy 服务器的文件筛选应用程序。

为此，您可以为 Storage Virtual Machine （ SVM ）配置两个单独的 FPolicy 策略，其中一个策略配置为阻止原生文件，另一个策略配置为基于 FPolicy 服务器的文件筛选。

- 原生文件阻止功能仅根据扩展名而不是文件内容对文件进行筛选。
- 对于符号链接，原生文件阻止使用根文件的文件扩展名。

了解更多信息 "[FPolicy：原生 文件阻止](#)"。

何时创建使用外部 FPolicy 服务器的配置

使用外部 FPolicy 服务器处理和管理通知的 FPolicy 配置可为需要基于文件扩展名进行简单文件阻止的使用情形提供强大的解决方案。

如果要执行以下操作，您应创建一个使用外部 FPolicy 服务器的配置：监控和记录文件访问事件，提供配额服务，根据简单文件扩展名以外的标准执行文件阻止，使用分层存储管理应用程序提供数据迁移服务，或者，提供一组细化策略，这些策略仅监控 Storage Virtual Machine （ SVM ）中的一部分数据。

ONTAP FPolicy 实施中的集群组件角色

集群，包含的 Storage Virtual Machine （ SVM ）和数据 LIF 都在 FPolicy 实施中发挥作用。

- * 集群 *

集群包含 FPolicy 管理框架，并维护和管理有关集群中所有 FPolicy 配置的信息。

- * SVM*

FPolicy 配置在 SVM 级别定义。此配置的范围是 SVM ，它仅在 SVM 资源上运行。一个 SVM 配置不能监控针对驻留在另一个 SVM 上的数据发出的文件访问请求并发送通知。

可以在管理 SVM 上定义 FPolicy 配置。在管理 SVM 上定义配置后，可以在所有 SVM 中查看和使用这些配

置。

- * 数据 LIF*

通过属于具有 FPolicy 配置的 SVM 的数据 LIF 连接到 FPolicy 服务器。用于这些连接的数据 LIF 可以按照用于正常客户端访问的数据 LIF 的方式进行故障转移。

ONTAP FPolicy 如何与外部 FPolicy 服务器配合使用

在 Storage Virtual Machine (SVM) 上配置并启用 FPolicy 后，FPolicy 将在 SVM 参与的每个节点上运行。FPolicy 负责与外部 FPolicy 服务器（FPolicy 服务器）建立和维护连接，处理通知以及管理与 FPolicy 服务器之间的通知消息。

此外，在连接管理中，FPolicy 还负责以下职责：

- 确保文件通知通过正确的 LIF 流向 FPolicy 服务器。
- 确保当多个 FPolicy 服务器与一个策略关联时，在向 FPolicy 服务器发送通知时会执行负载平衡。
- 在与 FPolicy 服务器的连接断开时尝试重新建立连接。
- 通过经过身份验证的会话向 FPolicy 服务器发送通知。
- 管理由 FPolicy 服务器建立的直通读取数据连接，以便在启用直通读取时为客户端请求提供服务。

如何使用控制通道进行 FPolicy 通信

FPolicy 会从 Storage Virtual Machine (SVM) 上参与的每个节点的数据 LIF 启动与外部 FPolicy 服务器的控制通道连接。FPolicy 使用控制通道传输文件通知；因此，根据 SVM 拓扑，FPolicy 服务器可能会看到多个控制通道连接。

如何将有权限的数据访问通道用于同步通信

对于同步使用情形，FPolicy 服务器会通过特权数据访问路径访问驻留在 Storage Virtual Machine (SVM) 上的数据。通过特权路径进行访问会将整个文件系统公开给 FPolicy 服务器。它可以访问数据文件来收集信息，扫描文件，读取文件或写入文件。

由于外部 FPolicy 服务器可以通过有权限的数据通道从 SVM 的根目录访问整个文件系统，因此有权限的数据通道连接必须安全。

FPolicy 连接凭据如何用于有权限的数据访问通道

FPolicy 服务器使用随 FPolicy 配置一起保存的特定 Windows 用户凭据来与集群节点建立有权限的数据访问连接。SMB 是唯一支持建立有权限的数据访问通道连接的协议。

如果 FPolicy 服务器需要特权数据访问，则必须满足以下条件：

- 集群上必须启用 SMB 许可证。
- FPolicy 服务器必须在 FPolicy 配置中配置的凭据下运行。

建立数据通道连接时，FPolicy 会使用凭据作为指定的 Windows 用户名。通过管理共享 ontap_admin\$ 进行数据访问。

为有权限的数据访问授予超级用户凭据的含义

ONTAP 使用在 FPolicy 配置中配置的 IP 地址和用户凭据的组合向 FPolicy 服务器授予超级用户凭据。

当 FPolicy 服务器访问数据时，超级用户状态会授予以下权限：

- 避免权限检查

用户可避免检查文件和目录访问。

- 特殊锁定权限

无论现有锁定如何，ONTAP 都允许对任何文件进行读取、写入或修改访问。如果 FPolicy 服务器对文件执行字节范围锁定，则会立即删除文件上的现有锁定。

- 绕过任何 FPolicy 检查

访问不会生成任何 FPolicy 通知。

FPolicy 如何管理策略处理

可能会为 Storage Virtual Machine (SVM) 分配多个 FPolicy 策略；每个策略的优先级各不相同。要在 SVM 上创建适当的 FPolicy 配置，请务必了解 FPolicy 如何管理策略处理。

系统会对每个文件访问请求进行初始评估，以确定哪些策略正在监控此事件。如果是受监控事件，则有关受监控事件的信息以及相关策略将传递到 FPolicy，并在其中对其进行评估。系统将按分配的优先级顺序评估每个策略。

配置策略时，应考虑以下建议：

- 如果您希望某个策略始终在评估其他策略之前进行评估，请为该策略配置较高的优先级。
- 如果对受监控事件成功执行请求的文件访问操作是根据另一策略评估文件请求的前提条件，请为控制第一个文件操作成功或失败的策略指定较高的优先级。

例如，如果一个策略管理 FPolicy 文件归档和还原功能，而另一个策略管理联机文件的文件访问操作，管理文件还原的策略必须具有较高的优先级，以便在允许第二个策略管理的操作之前还原文件。

- 如果要评估可能应用于文件访问操作的所有策略，请为同步策略指定较低的优先级。

您可以通过修改策略序列号对现有策略的策略优先级重新排序。但是，要让 FPolicy 根据修改后的优先级顺序评估策略，您必须禁用并重新启用此策略并使用修改后的序列号。

节点到外部 ONTAP FPolicy 服务器通信过程

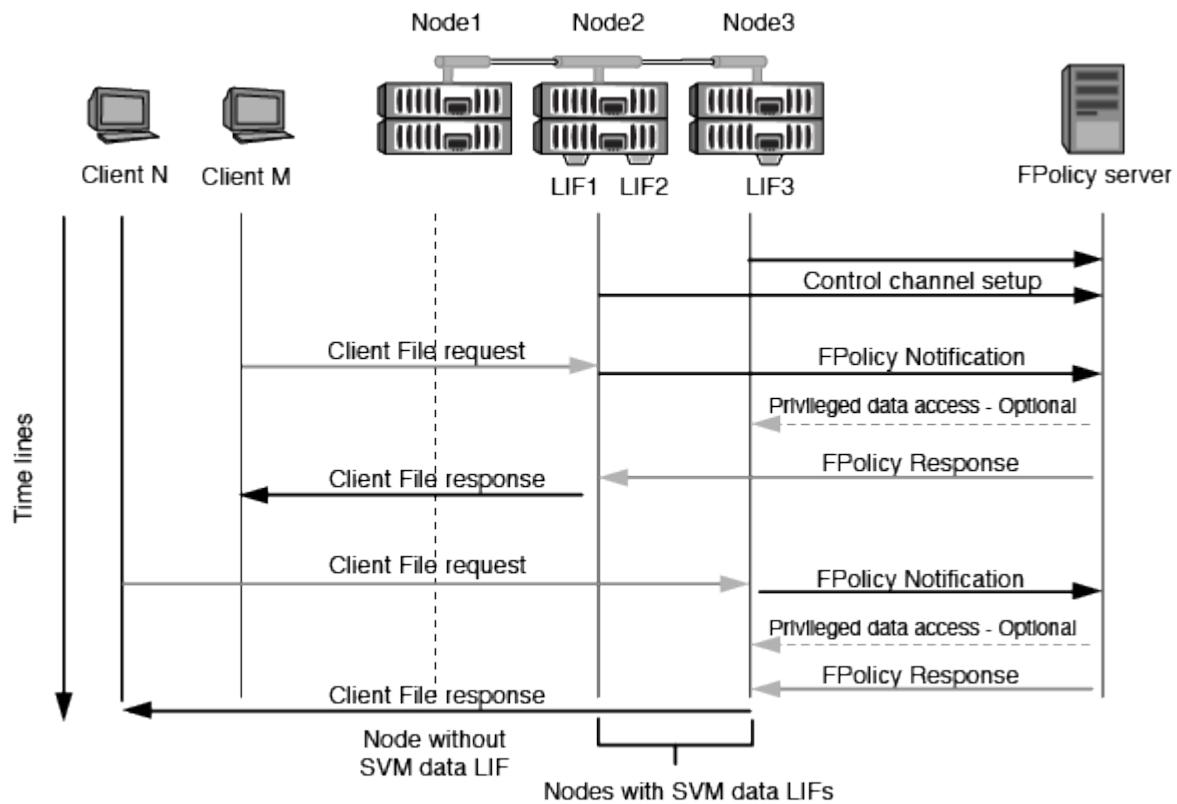
要正确规划 FPolicy 配置，您应了解节点到外部 FPolicy 服务器的通信过程是什么。

参与每个 Storage Virtual Machine (SVM) 的每个节点都会使用 TCP/IP 启动与外部 FPolicy 服务器 (FPolicy 服务器) 的连接。与 FPolicy 服务器的连接使用节点数据 LIF 进行设置；因此，只有当节点具有 SVM 的可操作数据 LIF 时，参与节点才能设置连接。

启用此策略后，参与节点上的每个 FPolicy 进程都会尝试与 FPolicy 服务器建立连接。它使用策略配置中指定的 FPolicy 外部引擎的 IP 地址和端口。

此连接将通过数据 LIF 从每个 SVM 上参与的每个节点建立一个控制通道，并连接到 FPolicy 服务器。此外，如果 IPv4 和 IPv6 数据 LIF 地址位于同一参与节点上，则 FPolicy 会尝试为 IPv4 和 IPv6 建立连接。因此，如果 SVM 扩展到多个节点，或者同时存在 IPv4 和 IPv6 地址，则在 SVM 上启用 FPolicy 策略后，FPolicy 服务器必须已准备好处理来自集群的多个控制通道设置请求。

例如，如果集群有三个节点：节点 1，节点 2 和节点 3，并且 SVM 数据 LIF 仅分布在节点 2 和节点 3 上，则无论数据卷的分布如何，控制通道只会从节点 2 和节点 3 启动。假设 Node2 有两个属于 SVM 的数据 LIF - LIF1 和 LIF2，并且初始连接来自 LIF1。如果 LIF1 发生故障，FPolicy 将尝试从 LIF2 建立控制通道。



FPolicy 如何在 LIF 迁移或故障转移期间管理外部通信

数据 LIF 可以迁移到同一节点中的数据端口或远程节点上的数据端口。

当数据 LIF 发生故障转移或迁移时，将与 FPolicy 服务器建立新的控制通道连接。然后，FPolicy 可以重试超时的 SMB 和 NFS 客户端请求，从而向外部 FPolicy 服务器发送新通知。节点拒绝 FPolicy 服务器对初始超时 SMB 和 NFS 请求的响应。

FPolicy 如何在节点故障转移期间管理外部通信

如果托管用于 FPolicy 通信的数据端口的集群节点发生故障，ONTAP 将中断 FPolicy 服务器与节点之间的连接。

可以通过配置故障转移策略将 FPolicy 通信中使用的数据端口迁移到另一个活动节点来缓解向 FPolicy 服务器进行集群故障转移所产生的影响。迁移完成后，将使用新的数据端口建立新的连接。

如果未将故障转移策略配置为迁移数据端口，则 FPolicy 服务器必须等待故障节点启动。节点启动后，将使用新会话 ID 从该节点启动新连接。



FPolicy 服务器检测到连接断开并显示 Keep-alive 协议消息。清除会话 ID 的超时时间是在配置 FPolicy 时确定的。默认的保活超时为 2 分钟。

了解跨 SVM 命名空间的 ONTAP FPolicy 服务

ONTAP 提供了一个统一的 Storage Virtual Machine (SVM) 命名空间。集群中的卷通过接合连接在一起，以提供一个逻辑文件系统。FPolicy 服务器可以识别命名空间拓扑，并在命名空间中提供 FPolicy 服务。

此命名空间是 SVM 特有的，并且包含在 SVM 中；因此，您只能从 SVM 上下文中查看此命名空间。命名空间具有以下特征：

- 每个 SVM 中都有一个命名空间，命名空间的根是根卷，在命名空间中以斜杠 (/) 表示。
- 所有其他卷的接合点均位于根 (/) 下方。
- 卷接合对客户端是透明的。
- 一个 NFS 导出可以提供对整个命名空间的访问；否则，导出策略可以导出特定卷。
- SMB 共享可以在卷或卷中的 qtree 上创建，也可以在命名空间中的任何目录上创建。
- 命名空间架构非常灵活。

典型命名空间架构的示例如下：

- 根下具有一个分支的命名空间
- 一个命名空间，其中包含多个根下的分支
- 一个命名空间，其中包含多个从根部断开的卷

ONTAP FPolicy 直通读取如何增强分层存储管理的可用性

通过直通读取，FPolicy 服务器（用作分层存储管理 (HSM) 服务器）可以对脱机文件进行读取访问，而无需将文件从二级存储系统重新调用到主存储系统。

如果将 FPolicy 服务器配置为向 SMB 服务器上的文件提供 HSM，则会发生基于策略的文件迁移，其中，文件脱机存储在二级存储上，而只有存根文件保留在主存储上。即使存根文件在客户端中显示为普通文件，但它实际上是一个与原始文件大小相同的稀疏文件。稀疏文件设置了 SMB 脱机位、并指向已迁移到二级存储的实际文件。

通常，在收到脱机文件的读取请求时，必须将请求的内容重新调用回主存储，然后通过主存储进行访问。需要将数据重新调用回主存储会产生一些不希望出现的影响。其中一个不希望受到的影响是，由于需要在响应请求之前重新调用内容，客户端请求的延迟增加，并且主存储上重新调用的文件所需的空间消耗增加。

通过 FPolicy 直通读取，HSM 服务器（FPolicy 服务器）可以对已迁移的脱机文件提供读取访问，而无需将文件从二级存储系统重新调用到主存储系统。可以直接从二级存储处理读取请求，而不是将文件重新调用回主存储。



FPolicy 直通读取操作不支持副本卸载 (ODX)。

直通读取通过提供以下优势增强了可用性：

- 即使主存储没有足够的空间将请求的数据重新调用回主存储，也可以处理读取请求。
- 当数据重新调用可能激增时，例如脚本或备份解决方案需要访问多个脱机文件时，可以更好地管理容量和性能。
- 可以处理快照中脱机文件的读取请求。

由于快照是只读的、因此、如果存根文件位于快照中、则 FPolicy 服务器无法还原原始文件。使用直通读取可消除此问题。

- 可以设置策略来控制何时通过访问二级存储上的文件来处理读取请求，以及何时应将脱机文件重新调用到主存储。

例如，可以在 HSM 服务器上创建一个策略，用于指定在将脱机文件迁移回主存储之前的指定时间段内可以访问该文件的次数。此类策略可避免调用很少访问的文件。

启用 **FPolicy** 直通读取时如何管理读取请求

您应了解启用 FPolicy 直通读取时如何管理读取请求，以便以最佳方式配置 Storage Virtual Machine (SVM) 和 FPolicy 服务器之间的连接。

启用 FPolicy 直通读取后，如果 SVM 收到脱机文件请求，则 FPolicy 将通过标准连接通道向 FPolicy 服务器 (HSM 服务器) 发送通知。

收到通知后，FPolicy 服务器将从通知中发送的文件路径读取数据，并通过 SVM 与 FPolicy 服务器之间建立的直通读取特权数据连接将请求的数据发送到 SVM。

发送数据后，FPolicy 服务器将对读取请求做出响应，即允许或拒绝。根据读取请求是被允许还是被拒绝，ONTAP 会向客户端发送请求的信息或错误消息。

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，这可能会影响 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
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GoogleProtobuf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。	-vserver vserver_name 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。

<p>引擎名称 _</p> <p>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。</p> <p>此名称最长可为 256 个字符。</p> <p> 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。</p> <p>此名称可以包含以下 ASCII 范围字符的任意组合：</p> <ul style="list-style-type: none"> • a 到 z • A 到 Z • 0 到 9 • “_”、“-”，and “.`Ω” 	<pre>-engine-name engine_name</pre>
<p>_ 主 FPolicy 服务器 _</p> <p>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。</p> <p>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。</p> <p>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。</p>	<pre>-primary-servers IP_address,</pre>
<p>端口号 _</p> <p>指定 FPolicy 服务的端口号。</p>	<pre>-port integer</pre>
<p>二级 FPolicy 服务器 _</p> <p>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。</p> <p>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。</p>	<pre>-secondary-servers IP_address,</pre>

<p>外部引擎类型 _</p> <p>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。</p> <p>设置为时 <code>synchronous</code>，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。</p> <p>设置为时 <code>asynchronous</code>，文件请求处理会向FPolicy服务器发送通知，然后继续。</p>	<p><code>-extern-engine-type</code> <code>external_engine_type</code> 此参数的值可以是以下值之一：</p> <ul style="list-style-type: none"> • <code>synchronous</code> • <code>asynchronous</code>
<p>外部引擎格式_</p> <p>指定外部引擎格式是xml还是protobuf。</p> <p>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。</p>	<p><code>-extern-engine-format</code> <code>{protobuf 或 xml}</code></p>
<p>用于与 FPolicy server_ 通信的 _ssl 选项</p> <p>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：</p> <ul style="list-style-type: none"> • 设置为时 <code>no-auth</code>，则不进行身份验证。 通信链路通过 TCP 建立。 • 设置为时 <code>server-auth</code>， 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 <code>mutual-auth</code>， 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。 <p>如果选择配置相互SSL身份验证、则还必须配置 <code>-certificate-common-name</code>, <code>-certificate-serial</code>, 和 <code>-certificate-ca-parameters</code></p>	<p><code>-ssl-option {no-auth}</code></p>
<p>server-auth</p> <p>证书 FQDN 或自定义公用名 _</p> <p>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。</p> <p>如果指定 <code>mutual-auth</code>。 <code>-ssl-option</code> 参数、则必须为指定一个值 <code>-certificate-common-name</code> 参数。</p>	<p><code>mutual-auth}</code></p> <p><code>-certificate-common-name text</code></p>

证书序列号 _	-certificate-serial text
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。	

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 _	-reqs-cancel-timeout integer[h]
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。	
m	s]
中止请求时超时 _	-reqs-abort-timeout `integer[h]
以小时为单位指定超时 (h)、分钟 (m)或秒 (s) 以便请求发生abording。 此值的范围为 0 到 200。	
m	s]

发送状态请求的间隔 _		-status-req-interval integer[h]
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。		
m	s]	
FPolicy 服务器上的最大未处理请求数 _		-max-server-reqs integer
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。		
断开无响应 FPolicy 服务器的超时 _		-server-progress -timeout integer[h]
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。		
m	s]	
向 FPolicy 服务器发送保活消息的 _Interval		-keep-alive-interval- integer[h]
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。		
m	s]	
最大重新连接尝试次数 _		-max-connection-retries integer
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。		

<p>接收缓冲区大小 _</p> <p>指定 FPolicy 服务器的已连接套接字的接收缓冲区大小。</p> <p>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。</p> <p>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）。</p>	<pre>-recv-buffer-size integer</pre>
<p>发送缓冲区大小 _</p> <p>指定 FPolicy 服务器的已连接套接字的发送缓冲区大小。</p> <p>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。</p> <p>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）。</p>	<pre>-send-buffer-size integer</pre>
<p>_Timeout，用于在重新连接期间清除会话 ID</p> <p>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。</p> <p>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。</p> <p>默认值设置为10秒。</p>	<pre>-session-timeout [integerh][integerm][integer秒]</pre>

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。	<code>-vserver vserver_name</code>
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： <ul style="list-style-type: none">• a 到 z• A 到 Z• 0 到 9• " _ "、" - "，and " `Ω "	<code>-event-name event_name</code>

_ 协议 _

-protocol protocol

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。

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

-filters filter, ...

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

是否需要执行卷操作 _	-volume-operation {true}
指定卷挂载和卸载操作是否需要监控。默认值为 false。	
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： <ul style="list-style-type: none">• 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

<p>策略名称 _</p> <p>指定 FPolicy 策略的名称。</p> <p>此名称最长可为 256 个字符。</p> <p> 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。</p> <p>此名称可以包含以下 ASCII 范围字符的任意组合：</p> <ul style="list-style-type: none"> • a 到 z • A 到 Z • 0 到 9 • “_”、“-”，and “.`Ω” 	<p>-policy-name policy_name</p>	<p>是的。</p>	<p>无</p>
<p>事件名称 _</p> <p>指定要与 FPolicy 策略关联的事件的逗号分隔列表。</p> <ul style="list-style-type: none"> • 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。 	<p>-events event_name, ...</p>	<p>是的。</p>	<p>无</p>
<p>持久性存储</p> <p>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。</p>	<p>-persistent -store persistent_store_name</p>	<p>否</p>	<p>无</p>

<p>外部引擎名称 _</p> <p>指定要与 FPolicy 策略关联的外部引擎的名称。</p> <ul style="list-style-type: none"> 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。 	<pre>-engine engine_name</pre>	<p>是（除非策略使用内部 ONTAP 原生引擎）</p>	native
<p><i>Is mandatory screening required</i></p> <p>指定是否需要强制文件访问筛选。</p> <ul style="list-style-type: none"> 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。 	<pre>-is-mandatory {true false}</pre>		否

true	<p><i>allow privileged access</i></p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>-allow -privileged -access {yes no}</p>
否 (除非启用直通读取)	<p>no</p> <p>特权用户名 _</p> <p>指定 FPolicy 服务器用于特权数据访问的帐户的用户名。</p> <ul style="list-style-type: none"> 此参数的值应采用 domain\user name 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。 	<p>-privileged -user-name user_name</p>

否（除非启用了特权访问）	无	<p><i>allow passthrough-read</i></p> <p>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：</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <ul style="list-style-type: none"> • 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。
--------------	---	--

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：

 在配置要在范围内包括或排除的共享、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	-vserver vserver_name
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。	
策略名称 _	-policy-name policy_name
指定要将范围附加到的 FPolicy 策略的名称。 FPolicy 策略必须已存在。	
要包含的共享 _	-shares-to-include share_name, ...
指定要监控应用范围的 FPolicy 策略的共享列表，以逗号分隔。	
要排除的共享 _	-shares-to-exclude share_name, ...
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。	
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 _	-volumes-to-exclude volume_name, ...
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。	
导出要包含的策略 _	-export-policies-to -include export_policy_name, ...
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。	
导出要排除的策略 _	-export-policies-to -exclude export_policy_name, ...
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。	
要包含的文件扩展名 _	-file-extensions-to -include file_extensions , ...
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。	
要排除的文件扩展名 _	-file-extensions-to -exclude file_extensions , ...
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。	

<p>目录上的文件扩展名检查是否已启用? <code>_</code></p> <p>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 <code>true</code>, 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 <code>false</code>, 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。</p> <p>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 <code>true</code>。</p>	<code>-is-file-extension -check-on-directories -enabled{true`我们可以为您提供 `false`}</code>
---	---

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		

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

- 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
```

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

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 Operation
	Name	Protocols	Operations	Filters	
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 KB = ~32 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

管理 FPolicy 配置

修改 FPolicy 配置

在 ONTAP 中修改 FPolicy 配置的命令

您可以通过修改构成 FPolicy 配置的元素来修改 FPolicy 配置。您可以修改外部引擎、FPolicy事件、FPolicy范围、FPolicy永久性存储和FPolicy策略。您还可以启用或禁用 FPolicy 策略。禁用 FPolicy 策略后，该策略的文件监控将停止。

您应先禁用 FPolicy 策略、然后再修改其配置。

要修改的内容	使用此命令 ...
外部引擎	vserver fpolicy policy external-engine modify
事件	vserver fpolicy policy event modify
范围	vserver fpolicy policy scope modify
永久性存储	vserver fpolicy persistent-store modify
策略	vserver fpolicy policy modify

有关的详细信息 vserver fpolicy policy，请参见["ONTAP 命令参考"](#)。

启用或禁用 ONTAP FPolicy 策略

配置完成后，您可以启用 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。如果要停止对策略的文件访问监控，可以禁用 FPolicy 策略。

开始之前

启用 FPolicy 策略之前，必须完成 FPolicy 配置。

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。

- 如果要更改 FPolicy 策略的优先级，必须禁用该策略，然后使用新序列号重新启用它。

步骤

- 执行相应的操作：

如果您要 ...	输入以下命令 ...
启用 FPolicy 策略	vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer
禁用 FPolicy 策略	vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name

显示有关 FPolicy 配置的信息

了解 ONTAP FPolicy 显示命令

在显示有关 FPolicy 配置的信息以了解如何配置时、这将非常有用 show 命令有效。

答 show 不带其他参数的命令以摘要形式显示信息。此外、每 show 命令具有两个相同的互斥可选参数：-instance 和 -fields。

使用时 -instance 参数、带 show 命令、则命令输出将以列表格式显示详细信息。在某些情况下，详细输出可能会很长，并且包含的信息可能比您需要的更多。您可以使用 -fieldsfieldname[,fieldname...] 参数、用于自定义输出、使其仅显示指定字段的信息。您可以通过输入来标识您可以指定的字段？之后 -fields 参数。



的输出 show 命令 -fields 参数可能会显示与请求的字段相关的其他必需字段。

每 show command 具有一个或多个可选参数、用于筛选该输出、并可用于缩小命令输出中显示的信息范围。您可以通过输入来确定哪些可选参数可用于命令？之后 show 命令：

。 show command 支持 UNIX 模式和通配符、可用于匹配命令参数中的多个值。例如，您可以在指定值时使用通配符（*），NOT 运算符（!），OR 运算符（=），范围运算符（integer...integer），小于运算符（<），大于运算符（>），小于或等于运算符（<=）以及大于或等于运算符（>=）。

有关使用 UNIX 模式和通配符的详细信息、请参见 [使用 ONTAP 命令行界面](#)。

用于显示 ONTAP 中 FPolicy 配置信息的命令

您可以使用 fpolicy show 用于显示有关 FPolicy 配置的信息的命令、包括有关 FPolicy 外部引擎、事件、范围和策略的信息。

要显示有关 FPolicy... 的信息	使用此命令 ...
外部引擎	vserver fpolicy policy external-engine show

事件	vserver fpolicy policy event show
范围	vserver fpolicy policy scope show
策略	vserver fpolicy policy show

有关的详细信息 vserver fpolicy policy，请参见["ONTAP 命令参考"](#)。

显示有关 FPolicy 策略状态的信息

您可以显示有关 FPolicy 策略状态的信息，以确定策略是否已启用，配置为使用的外部引擎，策略的序列号以及与 FPolicy 策略关联的 Storage Virtual Machine（SVM）。

关于此任务

如果未指定任何参数，则此命令将显示以下信息：

- SVM name
- Policy name
- 策略序列号
- 策略状态

除了显示集群或特定 SVM 上配置的 FPolicy 策略的策略状态信息之外，您还可以使用命令参数按其他条件筛选命令的输出。

您可以指定 -instance 用于显示有关列出策略的详细信息的参数。或者、您也可以使用 -fields 参数以仅显示命令输出中指示的字段、或 -fields ? 以确定您可以使用哪些字段。

步骤

1. 使用相应命令显示有关 FPolicy 策略状态的筛选信息：

要显示有关策略的状态信息的信息	输入命令 ...
在集群上	vserver fpolicy show
具有指定状态的 off`	`vserver fpolicy show -status {on
vserver fpolicy show -vserver vserver_name	在指定的 SVM 上 使用指定的策略名称
vserver fpolicy show -policy-name policy_name	使用指定外部引擎的

示例

以下示例显示了有关集群上 FPolicy 策略的信息：

cluster1::> vserver fpolicy show				
Vserver	Policy Name	Sequence Number	Status	Engine
FPolicy	cserver_policy	-	off	eng1
vs1.example.com	v1p1	-	off	eng2
vs1.example.com	v1p2	-	off	native
vs1.example.com	v1p3	-	off	native
vs1.example.com	cserver_policy	-	off	eng1
vs2.example.com	v1p1	3	on	native
vs2.example.com	v1p2	1	on	eng3
vs2.example.com	cserver_policy	2	on	eng1

显示有关已启用的 ONTAP FPolicy 策略的信息

您可以显示有关已启用 FPolicy 策略的信息，以确定配置为使用的 FPolicy 外部引擎，策略的优先级以及 FPolicy 策略与哪个 Storage Virtual Machine (SVM) 关联。

关于此任务

如果未指定任何参数，则此命令将显示以下信息：

- SVM name
- Policy name
- 策略优先级

您可以使用命令参数按指定条件筛选命令的输出。

步骤

1. 使用相应的命令显示有关已启用的 FPolicy 策略的信息：

要显示有关已启用策略的信息 ...	输入命令 ...
在集群上	vserver fpolicy show-enabled
在指定的 SVM 上	vserver fpolicy show-enabled -vserver vserver_name
使用指定的策略名称	vserver fpolicy show-enabled -policy-name policy_name
具有指定的序列号	vserver fpolicy show-enabled -priority integer

示例

以下示例显示了有关集群上已启用的 FPolicy 策略的信息：

Vserver	Policy Name	Priority
vs1.example.com	pol_native	native
vs1.example.com	pol_native2	native
vs1.example.com	pol1	2
vs1.example.com	pol2	4

管理 FPolicy 服务器连接

连接到ONTAP中的外部FPolicy服务器

要启用文件处理，如果先前已终止连接，则可能需要手动连接到外部 FPolicy 服务器。达到服务器超时后或由于某些错误，连接将终止。或者，管理员也可以手动终止连接。

关于此任务

如果发生致命错误，则可以终止与 FPolicy 服务器的连接。解决导致致命错误的问题描述后，您必须手动重新连接到 FPolicy 服务器。

步骤

1. 使用连接到外部FPolicy服务器 vserver fpolicy engine-connect 命令：

有关的详细信息 vserver fpolicy engine-connect，请参见["ONTAP 命令参考"](#)。

2. 使用验证外部FPolicy服务器是否已连接 vserver fpolicy show-engine 命令：

有关的详细信息 vserver fpolicy show-engine，请参见["ONTAP 命令参考"](#)。

在ONTAP中断开与外部FPolicy服务器的连接

您可能需要手动断开与外部 FPolicy 服务器的连接。如果 FPolicy 服务器在处理通知请求时出现问题，或者您需要对 FPolicy 服务器执行维护，则可能需要执行此操作。

步骤

1. 使用断开与外部FPolicy服务器的连接 vserver fpolicy engine-disconnect 命令：

有关的详细信息 vserver fpolicy engine-disconnect，请参见["ONTAP 命令参考"](#)。

2. 使用验证外部FPolicy服务器是否已断开连接 vserver fpolicy show-engine 命令：

有关的详细信息 vserver fpolicy show-engine，请参见["ONTAP 命令参考"](#)。

显示有关与外部 ONTAP FPolicy 服务器的连接的信息

您可以显示有关与集群或指定 Storage Virtual Machine (SVM) 的外部 FPolicy 服务器 (FPolicy 服务器) 连接的状态信息。此信息可帮助您确定连接了哪些 FPolicy 服务器。

关于此任务

如果未指定任何参数，则此命令将显示以下信息：

- SVM name
- Node name
- FPolicy policy name
- FPolicy 服务器 IP 地址
- FPolicy 服务器状态
- FPolicy 服务器类型

除了显示有关集群或特定 SVM 上的 FPolicy 连接的信息之外，您还可以使用命令参数按其他条件筛选命令的输出。

您可以指定 `-instance` 用于显示有关列出策略的详细信息的参数。或者、您也可以使用 `-fields` 参数、以便在命令输出中仅显示指示的字段。您可以输入 ? 之后 `-fields` 用于确定可以使用哪些字段的参数。

步骤

1. 使用相应的命令显示有关节点与 FPolicy 服务器之间连接状态的筛选信息：

要显示有关 FPolicy 服务器的连接状态信息 ...	输入 ...
您指定的	<code>vserver fpolicy show-engine -server IP_address</code>
指定的 SVM	<code>vserver fpolicy show-engine -vserver vserver_name</code>
附加了指定策略的	<code>vserver fpolicy show-engine -policy-name policy_name</code>
指定的服务器状态	<code>vserver fpolicy show-engine -server-status status</code> 服务器状态可以是以下状态之一： <ul style="list-style-type: none">• connected• disconnected• connecting• disconnecting

指定类型	<pre>vserver fpolicy show-engine -server-type type</pre> <p>FPolicy 服务器类型可以是以下类型之一：</p> <ul style="list-style-type: none"> • primary • secondary
已因指定原因断开连接的	<pre>vserver fpolicy show-engine -disconnect-reason text</pre> <p>断开连接的原因可能有多种。以下是断开连接的常见原因：</p> <ul style="list-style-type: none"> • Disconnect command received from CLI. • Error encountered while parsing notification response from FPolicy server. • FPolicy Handshake failed. • SSL handshake failed. • TCP Connection to FPolicy server failed. • The screen response message received from the FPolicy server is not valid.

示例

此示例显示了有关 SVM vs1.example.com 上 FPolicy 服务器的外部引擎连接的信息：

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy
      Server-      Server-
Vserver   Policy    Node     Server   status   type
-----  -----
-----  -----
vs1.example.com policy1  node1      10.1.1.2  connected  primary
vs1.example.com policy1  node1      10.1.1.3  disconnected  primary
vs1.example.com policy1  node2      10.1.1.2  connected  primary
vs1.example.com policy1  node2      10.1.1.3  disconnected  primary
```

此示例仅显示有关已连接 FPolicy 服务器的信息：

```

cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node      vserver          policy-name server
-----
node1    vs1.example.com  policy1     10.1.1.2
node2    vs1.example.com  policy1     10.1.1.2

```

显示有关 ONTAP FPolicy 直通读取连接状态的信息

您可以显示有关与集群或指定 Storage Virtual Machine (SVM) 的外部 FPolicy 服务器 (FPolicy 服务器) 的 FPolicy 直通读取连接状态的信息。此信息可帮助您确定哪些 FPolicy 服务器具有直通读取数据连接，以及哪些 FPolicy 服务器的直通读取连接已断开。

关于此任务

如果未指定任何参数，则此命令将显示以下信息：

- SVM name
- FPolicy policy name
- Node name
- FPolicy 服务器 IP 地址
- FPolicy 直通读取连接状态

除了显示有关集群或特定 SVM 上的 FPolicy 连接的信息之外，您还可以使用命令参数按其他条件筛选命令的输出。

您可以指定 `-instance` 用于显示有关列出策略的详细信息的参数。或者、您也可以使用 `-fields` 参数、以便在命令输出中仅显示指示的字段。您可以输入 `?` 之后 `-fields` 用于确定可以使用哪些字段的参数。

步骤

1. 使用相应的命令显示有关节点与 FPolicy 服务器之间连接状态的筛选信息：

要显示连接状态信息的对象	输入命令 ...
集群的 FPolicy 直通读取连接状态	<code>vserver fpolicy show-passthrough-read-connection</code>
指定 SVM 的 FPolicy 直通读取连接状态	<code>vserver fpolicy show-passthrough-read-connection -vserver vserver_name</code>
指定策略的 FPolicy 直通读取连接状态	<code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name</code>
指定策略的详细 FPolicy 直通读取连接状态	<code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance</code>

指定状态的 FPolicy 直通读取连接状态	vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status 服务器状态可以是以下状态之一：
	<ul style="list-style-type: none"> • connected • disconnected

示例

以下命令显示有关集群上所有 FPolicy 服务器的直通读取连接的信息：

```
cluster1::> vserver fpolicy show-passthrough-read-connection
              FPolicy          Server
Vserver      Policy Name   Node       Server      Status
-----  -----  -----
-----  -----
vs2.example.com  pol_cifs_2    FPolicy-01  2.2.2.2      disconnected
vs1.example.com  pol_cifs_1    FPolicy-01  1.1.1.1      connected
```

以下命令显示有关在 "pol_cifs_1" 策略中配置的 FPolicy 服务器的直通读取连接的详细信息：

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance
                                         Node: FPolicy-01
                                         Vserver: vs1.example.com
                                         Policy: pol_cifs_1
                                         Server: 1.1.1.1
                                         Session ID of the Control Channel: 8cef052e-2502-11e3-
                                         88d4-123478563412
                                         Server Status: connected
                                         Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
                                         Time Passthrough Read Channel was Disconnected: -
                                         Reason for Passthrough Read Channel Disconnection: none
```

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。