了解FPolicy

ONTAP 9

NetApp
April 24, 2024

目录

了解FPolicy

什么是 FPolicy 解决方案的两个部分

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。

什么是同步和异步通知

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

FPolicy持久存储

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。

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。

最佳实践

集群管理员需要在启用了FPolicy的每个SVM上为永久性存储配置一个卷。配置后、永久性存储将捕获所有匹配的FPolicy事件、这些事件将在FPolicy管道中进行进一步处理并发送到外部服务器。

如果发生意外重新启动或FPolicy被禁用并再次启用、则持久存储将保持上次收到事件时的状态。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。

如果永久性存储卷从同一SVM中的一个节点移至另一个节点、则尚未处理的通知也将移至新节点。您需要重新运行 `fpolicy persistent-store create` 命令、以确保将待定通知传送到外部服务器。

永久性存储卷会按SVM进行设置。对于每个启用了FPolicy的SVM、您需要创建一个永久性存储卷。

在包含预期Fpolicy监控的最大流量的生命周期的节点上创建永久性存储卷。

如果持久性存储中累积的通知超过所配置卷的大小、FPolicy将开始删除传入通知并显示相应的EMS消息。

创建卷时指定的永久性存储卷名称和接合路径应匹配。

将Snapshot策略设置为 `none` 而不是 `default`。这是为了确保不会意外还原快照而导致当前事件丢失、并防止可能发生重复的事件处理。

使持久存储卷无法用于外部用户协议访问(CIFS或NFS)、以避免意外损坏或删除保留的事件记录。为此、在启用FPolicy后、请在ONTAP中卸载卷以删除接合路径、这样用户协议访问就无法访问该路径。

有关详细信息，请参见 "创建持久性存储"。

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。

集群组件在 **FPolicy** 实施中发挥的角色

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。

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。

什么是节点到外部 **FPolicy** 服务器通信过程

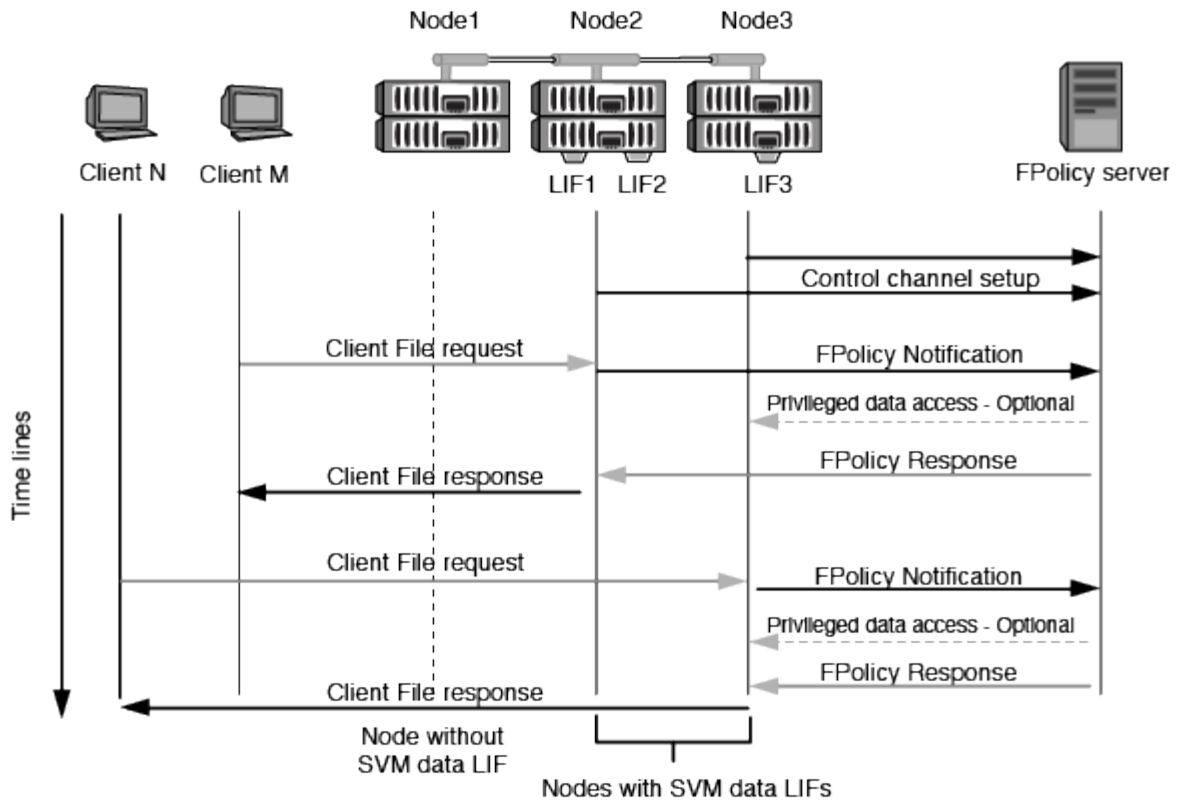
要正确规划 FPolicy 配置，您应了解节点到外部 FPolicy 服务器的通信过程是什么。

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。

FPolicy 服务如何跨 SVM 命名空间工作

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

FPolicy 直通读取如何提高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 Snapshot 副本中脱机文件的读取请求。

  由于 Snapshot 副本是只读的，因此，如果存根文件位于 Snapshot 副本中，则 FPolicy 服务器将无法还原原始文件。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。