# 规划 FPolicy 外部引擎配置

ONTAP 9

NetApp
May 09, 2024

# 目录

# 规划 FPolicy 外部引擎配置

## 规划 FPolicy 外部引擎配置

在配置 FPolicy 外部引擎（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

外部引擎配置定义了 FPolicy 在建立和管理与外部 FPolicy 服务器（ FPolicy 服务器）的连接时所需的信息，其中包括以下信息：

- 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
- 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*<br><br>指定要与此外部引擎关联的 SVM 名称。<br><br>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 _<br><br>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。<br><br>此名称最长可为 256 个字符。<br><br>ⓘ 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。<br><br>此名称可以包含以下 ASCII 范围字符的任意组合：<br><br>• a 到 z<br>• A 到 Z<br>• 0 到 9<br>• “_”、“-”, and "`.`Ω" | -engine-name engine_name |
| _ 主 FPolicy 服务器 _<br><br>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。<br><br>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。<br><br>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 _<br><br>指定 FPolicy 服务的端口号。 | -port integer |
| 二级 FPolicy 服务器 _<br><br>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。<br><br>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 _<br><br>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。<br><br>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。<br><br>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：<br><br>• `synchronous`<br>• `asynchronous` |
| 用于与 FPolicy server_ 通信的 _ssl 选项<br><br>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：<br><br>• 设置为时 `no-auth`，则不进行身份验证。<br><br>通信链路通过 TCP 建立。<br><br>• 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。<br>• 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。<br><br>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 _<br><br>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。<br><br>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 _<br><br>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。<br><br>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 _<br><br>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。<br><br>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 _<br><br>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。<br><br>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。<br><br>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 _<br><br>以小时为单位指定超时 (`h`)、分钟 (`m`)或秒 (`s`)以使请求发生abording。<br><br>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 _<br><br>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。<br><br>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 _<br><br>指定可在 FPolicy 服务器上排队的最大未处理请求数。<br><br>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 _<br><br>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。<br><br>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。<br><br>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<br><br>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。<br><br>保持活动消息会检测半打开的连接。<br><br>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 _<br><br>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。<br><br>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 _<br><br>指定 FPolicy 服务器的已连接套接字的接收缓冲区大小。<br><br>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。<br><br>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 _<br><br>指定 FPolicy 服务器的已连接套接字的发送缓冲区大小。<br><br>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。<br><br>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<br><br>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。<br><br>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。<br><br>默认值设置为10秒。 | `-session-timeout [integerh][integerm][integer秒]` |

# 追加信息关于配置 **FPolicy** 外部引擎以使用经过 **SSL** 身份验证的连接的信息

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 策略使用已安装的证书时，不能删除此证书。

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`。

## 证书不会在具有非 ID-preserve 配置的 SVM 灾难恢复关系中进行复制

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)。

## 具有 MetroCluster 和 SVM 灾难恢复配置的集群范围 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。

# 填写 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 | | |