# Planen Sie die Konfiguration der externen FPolicy Engine

ONTAP 9

NetApp
March 22, 2023

# Inhaltsverzeichnis

# Planen Sie die Konfiguration der externen FPolicy Engine

Bevor Sie die FPolicy External Engine (externe Engine) konfigurieren, müssen Sie verstehen, was es bedeutet, eine externe Engine zu erstellen und welche Konfigurationsparameter verfügbar sind. Anhand dieser Informationen können Sie festlegen, welche Werte für jeden Parameter festgelegt werden sollen.

## Informationen, die bei der Erstellung der externen FPolicy Engine definiert werden

Die Konfiguration der externen Engine definiert die Informationen, die FPolicy Verbindungen zu den externen FPolicy Servern (FPolicy-Servern) herstellen und verwalten muss, einschließlich der folgenden Informationen:

- SVM-Name
- Motorname
- Die IP-Adressen der primären und sekundären FPolicy Server und der zu verwendenden TCP-Portnummer für die Verbindung zu den FPolicy Servern
- Ob der Engine-Typ asynchron oder synchron ist
- Wie authentifiziert man die Verbindung zwischen dem Knoten und dem FPolicy-Server

  Wenn Sie die gegenseitige SSL-Authentifizierung konfigurieren, müssen Sie auch Parameter konfigurieren, die SSL-Zertifikatsinformationen bereitstellen.

- So verwalten Sie die Verbindung mit verschiedenen erweiterten Berechtigungseinstellungen

  Dazu gehören Parameter, die z. B. Timeout-Werte, Wiederholungswerte, Keep-Alive-Werte, maximale Anforderungswerte, Werte für gesendete und empfangbare Puffergrößen sowie Werte für Sitzungszeitüberschreitungen definieren.

Der `vserver fpolicy policy external-engine create` Mit dem Befehl wird eine FPolicy externe Engine erstellt.

## Was sind die grundlegenden externen Motorparameter

Sie können die folgende Tabelle mit grundlegenden FPolicy Konfigurationsparametern verwenden, um Ihre Konfiguration zu planen:

| Informationstyp | Option |
|---|---|

| | |
|---|---|
| *SVM*<br><br>Gibt den SVM-Namen an, den Sie mit dieser externen Engine verknüpfen möchten.<br><br>Jede FPolicy-Konfiguration ist innerhalb einer einzelnen SVM definiert. Die externe Engine, das Richtlinienereignis, der Richtlinienumfang und die Richtlinie, die gemeinsam eine FPolicy-Konfiguration erstellen, müssen mit derselben SVM verknüpft werden. | `-vserver vserver_name` |
| *Motorname*<br><br>Gibt den Namen an, der der externen Engine-Konfiguration zugewiesen werden soll. Sie müssen den Namen der externen Engine später angeben, wenn Sie die FPolicy erstellen. Dadurch wird die externe Engine mit der Richtlinie verknüpft.<br><br>Der Name kann bis zu 256 Zeichen lang sein.<br><br>Wenn Sie den Namen der externen Engine in einer Disaster-Recovery-Konfiguration von MetroCluster oder SVM konfigurieren, sollte der Name bis zu 200 Zeichen lang sein.<br><br>Der Name kann eine beliebige Kombination der folgenden Zeichen des ASCII-Bereichs enthalten:<br><br>• `a` Bis `z`<br>• `A` Bis `Z`<br>• `0` Bis `9`<br>• „_“,„-`", and ".`“ | `-engine-name engine_name` |
| *Primary FPolicy Server*<br><br>Gibt die primären FPolicy Server an, an die der Node Benachrichtigungen für eine bestimmte FPolicy sendet. Der Wert wird als kommagetrennte Liste von IP-Adressen angegeben.<br><br>Wenn mehr als eine IP-Adresse für den primären Server angegeben wird, erstellt jeder Node, an dem die SVM teilnimmt, eine Kontrollverbindung zu jedem angegebenen primären FPolicy-Server zum Zeitpunkt der Aktivierung der Richtlinie. Wenn Sie mehrere primäre FPolicy-Server konfigurieren, werden Benachrichtigungen nach Round Robin-Verfahren an die FPolicy-Server gesendet.<br><br>Wenn die externe Engine in einer MetroCluster- oder SVM-Disaster-Recovery-Konfiguration verwendet wird, sollten Sie die IP-Adressen der FPolicy-Server am Quellstandort als primäre Server angeben. Die IP-Adressen der FPolicy-Server am Zielstandort sollten als sekundäre Server angegeben werden. | `-primary-servers IP_address,...` |

| | |
|---|---|
| *Portnummer*<br><br>Gibt die Portnummer des FPolicy-Dienstes an. | `-port integer` |
| *Secondary FPolicy Server*<br><br>Gibt die sekundären FPolicy-Server an, an die Dateizugriffsereignisse für eine bestimmte FPolicy gesendet werden sollen. Der Wert wird als kommagetrennte Liste von IP-Adressen angegeben.<br><br>Sekundäre Server werden nur verwendet, wenn keiner der primären Server erreichbar ist. Verbindungen zu sekundären Servern werden hergestellt, wenn die Richtlinie aktiviert ist. Benachrichtigungen werden jedoch nur an sekundäre Server gesendet, wenn keiner der primären Server erreichbar ist. Wenn Sie mehrere sekundäre Server konfigurieren, werden Benachrichtigungen nach Round Robin-Verfahren an die FPolicy-Server gesendet. | `-secondary-servers IP_address,...` |
| *Externer Motortyp*<br><br>Gibt an, ob die externe Engine im synchronen oder asynchronen Modus arbeitet. FPolicy arbeitet standardmäßig im synchronen Modus.<br><br>Wenn eingestellt auf `synchronous`, Die Verarbeitung von Dateianfragen sendet eine Benachrichtigung an den FPolicy-Server, wird aber dann erst fortgesetzt, nachdem eine Antwort vom FPolicy-Server erhalten wurde. In diesem Punkt wird der Anforderungsfluss entweder fortgesetzt oder die Verarbeitung führt zu Denial-DoS, je nachdem, ob die Antwort vom FPolicy-Server die angeforderte Aktion zulässt.<br><br>Wenn eingestellt auf `asynchronous`, Die Verarbeitung von Dateianfragen sendet eine Benachrichtigung an den FPolicy-Server und wird dann fortgesetzt. | `-extern-engine-type external_engine_type` Der Wert für diesen Parameter kann einer der folgenden Werte sein:<br><br>• `synchronous`<br>• `asynchronous` |

| | |
|---|---|
| *SSL-Option zur Kommunikation mit FPolicy Server*<br><br>Gibt die SSL-Option für die Kommunikation mit dem FPolicy-Server an. Dies ist ein erforderlicher Parameter. Sie können eine der Optionen basierend auf den folgenden Informationen auswählen:<br><br>• Wenn eingestellt auf `no-auth`, Keine Authentifizierung erfolgt.<br><br>Die Kommunikationsverbindung wird über TCP hergestellt.<br><br>• Wenn eingestellt auf `server-auth`, Die SVM authentifiziert den FPolicy-Server mithilfe einer SSL-Server-Authentifizierung.<br>• Wenn eingestellt auf `mutual-auth`. Gegenseitige Authentifizierung erfolgt zwischen der SVM und dem FPolicy-Server. Die SVM authentifiziert den FPolicy-Server und der FPolicy-Server authentifiziert die SVM.<br><br>Wenn Sie die gegenseitige SSL-Authentifizierung konfigurieren, müssen Sie auch die konfigurieren `-certificate-common-name`, `-certificate-serial`, und `-certifcate-ca` Parameter. | `-ssl-option` {`no-auth` |
| `server-auth` | `mutual-auth`} |
| *Zertifikat FQDN oder benutzerdefinierter allgemeiner Name*<br><br>Gibt den Zertifikatsnamen an, der verwendet wird, wenn die SSL-Authentifizierung zwischen der SVM und dem FPolicy-Server konfiguriert ist. Sie können den Zertifikatnamen als FQDN oder als benutzerdefinierten gemeinsamen Namen angeben.<br><br>Wenn Sie angeben `mutual-auth` Für das `-ssl-option` Parameter. Sie müssen einen Wert für das angeben `-certificate-common-name` Parameter. | `-certificate-common -name` `text` |
| *Seriennummer des Zertifikats*<br><br>Gibt die Seriennummer des Zertifikats an, das für die Authentifizierung verwendet wird, wenn die SSL-Authentifizierung zwischen der SVM und dem FPolicy-Server konfiguriert ist.<br><br>Wenn Sie angeben `mutual-auth` Für das `-ssl-option` Parameter. Sie müssen einen Wert für das angeben `-certificate-serial` Parameter. | `-certificate-serial` `text` |
| *Zertifizierungsstelle*<br><br>Gibt den CA-Namen des Zertifikats an, das für die Authentifizierung verwendet wird, wenn die SSL-Authentifizierung zwischen der SVM und dem FPolicy-Server konfiguriert ist.<br><br>Wenn Sie angeben `mutual-auth` Für das `-ssl-option` Parameter. Sie müssen einen Wert für das angeben `-certificate-ca` Parameter. | `-certificate-ca` `text` |

# Was sind die erweiterten Optionen der externen Engine

Sie können die folgende Tabelle mit erweiterten FPolicy Konfigurationsparametern verwenden, wenn Sie planen, Ihre Konfiguration mit erweiterten Parametern anzupassen. Mit diesen Parametern ändern Sie das Kommunikationsverhalten zwischen den Cluster-Nodes und den FPolicy-Servern:

| Informationstyp | Option |
| --- | --- |
| *Timeout zum Abbrechen einer Anfrage*<br><br>Gibt das Zeitintervall in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Dass der Knoten auf eine Antwort vom FPolicy-Server wartet.<br><br>Wenn das Zeitüberschreitungsintervall abgelaufen ist, sendet der Node eine Anforderung zum Abbrechen an den FPolicy-Server. Der Node sendet dann die Benachrichtigung an einen alternativen FPolicy-Server. Dieses Timeout unterstützt den Umgang mit einem FPolicy-Server, der nicht reagiert, was die Reaktion von SMB/NFS-Clients verbessern kann. Das Abbrechen von Anfragen nach einem Timeout kann außerdem dazu beitragen, Systemressourcen freizugeben, da die Benachrichtigungsanfrage von einem heruntergedrückten/schlechten FPolicy-Server auf einen alternativen FPolicy-Server verschoben wird.<br><br>Der Bereich für diesen Wert ist `0` Bis `100`. Wenn der Wert auf festgelegt ist `0`, Die Option ist deaktiviert und Cancel Request Nachrichten werden nicht an den FPolicy-Server gesendet. Die Standardeinstellung lautet `20s`. | `-reqs-cancel-timeout integer`[H m m m V natürlich] |
| *Timeout für Abbruch einer Anfrage*<br><br>Gibt die Zeitüberschreitung in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Zum Abbruch einer Anfrage.<br><br>Der Bereich für diesen Wert ist `0` Bis `200`. | `-reqs-abort-timeout ` `integer`[H m m m V natürlich] |
| *Intervall für das Senden von Statusanforderungen*<br><br>Gibt das Intervall in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Nach dem eine Statusanforderung an den FPolicy-Server gesendet wird.<br><br>Der Bereich für diesen Wert ist `0` Bis `50`. Wenn der Wert auf festgelegt ist `0`, Die Option ist deaktiviert und Status Request Nachrichten werden nicht an den FPolicy-Server gesendet. Die Standardeinstellung lautet `10s`. | `-status-req-interval integer`[H m m m V natürlich] |
| *Maximale Anzahl ausstehende Anforderungen auf dem FPolicy-Server*<br><br>Gibt die maximale Anzahl der ausstehenden Anforderungen an, die auf dem FPolicy-Server in die Warteschlange gestellt werden können.<br><br>Der Bereich für diesen Wert ist `1` Bis `10000`. Die Standardeinstellung lautet `50`. | `-max-server-reqs integer` |

| | |
|---|---|
| *Timeout zum Trennen eines nicht ansprechenden FPolicy Servers*<br><br>Gibt das Zeitintervall in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Nach der die Verbindung zum FPolicy-Server beendet wird.<br><br>Die Verbindung wird nach dem Timeout-Zeitraum nur beendet, wenn die Warteschlange des FPolicy-Servers die maximal zulässigen Anforderungen enthält und innerhalb des Timeout-Zeitraums keine Antwort empfangen wird. Es gibt entweder eine maximal zulässige Anzahl von Anforderungen `50` (Die Standardeinstellung) oder die vom angegebene Zahl `max-server-reqs-` Parameter.<br><br>Der Bereich für diesen Wert ist `1` Bis `100`. Die Standardeinstellung lautet `60s`. | `-server-progress -timeout integer`[H m m m V natürlich] |
| *Intervall zum Senden von Keep-Alive-Nachrichten an den FPolicy-Server*<br><br>Gibt das Zeitintervall in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Bei denen Keep-Alive-Nachrichten an den FPolicy-Server gesendet werden.<br><br>Keep-Alive-Meldungen erkennen halboffene Verbindungen.<br><br>Der Bereich für diesen Wert ist `10` Bis `600`. Wenn der Wert auf festgelegt ist `0`, Die Option ist deaktiviert und Keep-Alive-Nachrichten werden nicht an die FPolicy-Server gesendet. Die Standardeinstellung lautet `120s`. | `-keep-alive-interval-integer`[H m m m V natürlich] |
| *Maximale Anzahl Verbindungsversuche*<br><br>Gibt die maximale Anzahl der Male an, die die SVM nach einer Verbindungsherstellung versucht, eine Verbindung zum FPolicy-Server herzustellen.<br><br>Der Bereich für diesen Wert ist `0` Bis `20`. Die Standardeinstellung lautet `5`. | `-max-connection-retries integer` |
| *Puffergröße empfangen*<br><br>Gibt die Empfangsbuffer-Größe des angeschlossenen Sockets für den FPolicy-Server an.<br><br>Der Standardwert ist 256 Kilobyte (KB). Wenn der Wert auf 0 gesetzt ist, wird die Größe des Empfangspuffers auf einen vom System definierten Wert gesetzt.<br><br>Wenn beispielsweise die Standard-Empfangspuffgröße des Sockets 65536 Byte beträgt, wird durch Setzen des einstellbaren Werts auf 0 die Socket-Puffergröße auf 65536 Byte gesetzt. Sie können einen beliebigen nicht-Standardwert verwenden, um die Größe (in Byte) des Empfangspuffers festzulegen. | `-recv-buffer-size integer` |

| | |
|---|---|
| *Puffergröße senden*<br><br>Gibt die Sendepuffer-Größe des angeschlossenen Sockets für den FPolicy-Server an.<br><br>Der Standardwert ist 256 Kilobyte (KB). Wenn der Wert auf 0 gesetzt ist, wird die Größe des Sendepuffers auf einen vom System definierten Wert gesetzt.<br><br>Wenn beispielsweise die Standard-Sendepuffer-Größe des Sockets auf 65536 Byte eingestellt ist, indem der einstellbare Wert auf 0 gesetzt wird, wird die Socket-Puffergröße auf 65536 Byte gesetzt. Sie können einen beliebigen nicht-Standardwert verwenden, um die Größe (in Bytes) des Sendepuffers festzulegen. | `-send-buffer-size integer` |
| *Timeout zum Löschen einer Sitzungs-ID während der erneuten Verbindung*<br><br>Gibt das Intervall in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Anschließend wird während der erneuten Verbindungsversuche eine neue Sitzungs-ID an den FPolicy-Server gesendet.<br><br>Wenn die Verbindung zwischen dem Speicher-Controller und dem FPolicy-Server beendet wird und eine erneute Verbindung innerhalb des hergestellt wird `-session-timeout` Intervall wird die alte Session-ID an den FPolicy Server gesendet, damit es Antworten für alte Benachrichtigungen senden kann.<br><br>Der Standardwert ist 10 Sekunden. | `-session-timeout [integerH][integerM][integerS]` |

# Weitere Informationen zum Konfigurieren von FPolicy-externen Engines zur Verwendung von SSL-authentifizierten Verbindungen

Sie müssen einige zusätzliche Informationen wissen, wenn Sie die FPolicy externe Engine konfigurieren möchten, um SSL bei der Verbindung zu FPolicy-Servern zu verwenden.

## SSL-Serverauthentifizierung

Wenn Sie die FPolicy-externe Engine für die SSL-Server-Authentifizierung konfigurieren, müssen Sie vor dem Erstellen der externen Engine das öffentliche Zertifikat der Zertifizierungsstelle (CA) installieren, die das FPolicy-Server-Zertifikat signiert hat.

## Gegenseitige Authentifizierung

Wenn Sie FPolicy externe Engines konfigurieren, um bei der Verbindung von Storage Virtual Machine (SVM)-Daten-LIFs mit externen FPolicy-Servern SSL gegenseitige Authentifizierung zu verwenden, bevor Sie die externe Engine erstellen, Sie müssen das öffentliche Zertifikat der CA installieren, die das FPolicy-Serverzertifikat unterzeichnet hat, sowie das öffentliche Zertifikat und die Schlüsseldatei zur Authentifizierung der SVM. Sie dürfen dieses Zertifikat nicht löschen, während alle FPolicy-Richtlinien das installierte Zertifikat

verwenden.

Wenn das Zertifikat gelöscht wird, während FPolicy es für gegenseitige Authentifizierung verwendet, wenn eine Verbindung zu einem externen FPolicy-Server hergestellt wird, können Sie eine deaktivierte FPolicy, die dieses Zertifikat verwendet, nicht aktivieren. Die FPolicy kann in dieser Situation nicht wieder aktiviert werden, auch wenn ein neues Zertifikat mit denselben Einstellungen erstellt und auf der SVM installiert wird.

Wenn das Zertifikat gelöscht wurde, müssen Sie ein neues Zertifikat installieren, neue FPolicy-externe Engines erstellen, die das neue Zertifikat verwenden, und die neuen externen Engines mit der FPolicy verknüpfen, die Sie durch Ändern der FPolicy erneut aktivieren möchten.

### Installieren Sie Zertifikate für SSL

Das öffentliche Zertifikat der CA, das zum Signieren des FPolicy-Server-Zertifikats verwendet wird, wird mithilfe der installiert `security certificate install` Befehl mit dem `-type` Parameter auf gesetzt `client_ca`. Der für die Authentifizierung der SVM erforderliche private Schlüssel und das öffentliche Zertifikat werden mithilfe des installiert `security certificate install` Befehl mit dem `-type` Parameter auf gesetzt `server`.

# Zertifikate replizieren sich in SVM Disaster-Recovery-Beziehungen nicht mit einer Konfiguration, die keine IDs enthält

Sicherheitszertifikate, die für die SSL-Authentifizierung verwendet werden, wenn Verbindungen zu FPolicy-Servern hergestellt werden, replizieren keine SVM-Disaster-Recovery-Ziele mit Konfigurationen, die keine ID-Preserve enthalten. Obwohl die externe FPolicy-Engine-Konfiguration auf der SVM repliziert wird, werden Sicherheitszertifikate nicht repliziert. Sie müssen die Sicherheitszertifikate manuell auf dem Ziel installieren.

Wenn Sie eine SVM Disaster-Recovery-Beziehung einrichten, wählen Sie den Wert für `-identity -preserve` Option des `snapmirror create` Der Befehl bestimmt die Konfigurationsdetails, die in der Ziel-SVM repliziert werden.

Wenn Sie die einstellen `-identity-preserve` Option auf `true` (ID-Preserve) werden alle FPolicy Konfigurationsdetails repliziert, einschließlich der Informationen zum Sicherheitszertifikat. Sie müssen die Sicherheitszertifikate nur auf dem Ziel installieren, wenn Sie die Option auf festlegen `false` (Nicht-ID-Preserve).

# Einschränkungen für externe Cluster-Scoped FPolicy Engines mit MetroCluster und SVM Disaster-Recovery-Konfigurationen

Sie können eine externe Cluster-Scoped FPolicy Engine erstellen, indem Sie die Cluster Storage Virtual Machine (SVM) der externen Engine zuweisen. Beim Erstellen einer externen Engine mit Cluster-Umfang in einer Disaster-Recovery-Konfiguration mit MetroCluster oder SVM gibt es jedoch bestimmte Einschränkungen bei der Auswahl der Authentifizierungsmethode, die die SVM für die externe Kommunikation mit dem FPolicy-Server verwendet.

Es gibt drei Authentifizierungsoptionen, die Sie bei der Erstellung von externen FPolicy-Servern wählen können: Keine Authentifizierung, SSL-Serverauthentifizierung und gegenseitige SSL-Authentifizierung. Obwohl die Auswahl der Authentifizierungsoption für den externen FPolicy-Server einer Daten-SVM nicht eingeschränkt ist, gibt es Einschränkungen bei der Erstellung einer externen Cluster-Scoped FPolicy Engine:

| Konfiguration | Erlaubt? |
|---|---|
| Disaster Recovery mit MetroCluster oder SVM und eine externe Cluster-FPolicy-Scoped-Engine ohne Authentifizierung (SSL ist nicht konfiguriert) | Ja. |
| Disaster Recovery für MetroCluster oder SVM und eine externe Cluster-FPolicy Scoped Engine mit SSL-Server oder gegenseitige SSL-Authentifizierung | Nein |

- Wenn eine externe Cluster-Scoped FPolicy Engine mit SSL-Authentifizierung vorhanden ist und Sie eine MetroCluster- oder SVM-Disaster-Recovery-Konfiguration erstellen möchten, müssen Sie diese externe Engine ändern, um keine Authentifizierung zu verwenden oder die externe Engine zu entfernen, bevor Sie die MetroCluster- oder SVM-Disaster Recovery-Konfiguration erstellen können.
- Falls die Disaster Recovery-Konfiguration von MetroCluster oder SVM bereits vorhanden ist, verhindert ONTAP die Erstellung einer externen FPolicy Engine mit Cluster-Umfang und SSL-Authentifizierung.

# Füllen Sie das Konfigurationsarbeitsblatt für die externe FPolicy Engine aus

Mit diesem Arbeitsblatt können Sie die Werte aufzeichnen, die Sie während der Konfiguration der externen FPolicy Engine benötigen. Wenn ein Parameterwert erforderlich ist, müssen Sie vor der Konfiguration der externen Engine festlegen, welchen Wert für diese Parameter verwendet werden soll.

## Informationen für eine grundlegende externe Engine-Konfiguration

Sie sollten aufzeichnen, ob Sie die einzelnen Parametereinstellungen in die externe Engine-Konfiguration aufnehmen möchten, und dann den Wert für die Parameter notieren, die Sie einbeziehen möchten.

| Informationstyp | Erforderlich | Einschließlich | Ihre Werte |
|---|---|---|---|
| Name der Storage Virtual Machine (SVM | Ja. | Ja. | |
| Motorname | Ja. | Ja. | |
| Primäre FPolicy-Server | Ja. | Ja. | |
| Port-Nummer | Ja. | Ja. | |
| Sekundäre FPolicy Server | Nein | | |
| Externer Motortyp | Nein | | |

| | | | |
|---|---|---|---|
| SSL-Option zur Kommunikation mit externem FPolicy-Server | Ja. | Ja. | |
| FQDN des Zertifikats oder benutzerdefinierter allgemeiner Name | Nein | | |
| Seriennummer des Zertifikats | Nein | | |
| Zertifizierungsstelle | Nein | | |

## Informationen für erweiterte externe Motorparameter

Um eine externe Engine mit erweiterten Parametern zu konfigurieren, müssen Sie den Konfigurationsbefehl im erweiterten Berechtigungsmodus eingeben.

| Informationstyp | Erforderlich | Einschließlich | Ihre Werte |
|---|---|---|---|
| Zeitüberschreitung beim Abbrechen einer Anfrage | Nein | | |
| Timeout beim Abbrechen einer Anfrage | Nein | | |
| Intervall für das Senden von Statusanforderungen | Nein | | |
| Maximale offene Anfragen auf dem FPolicy-Server | Nein | | |
| Timeout zum Trennen eines nicht ansprechenden FPolicy-Servers | Nein | | |
| Intervall für das Senden von Keep-Alive-Nachrichten an den FPolicy-Server | Nein | | |
| Maximale Anzahl von Verbindungsversuchen | Nein | | |
| Empfangspuffgröße | Nein | | |
| Puffergröße senden | Nein | | |
| Zeitüberschreitung beim Spülen einer Sitzungs-ID während der erneuten Verbindung | Nein | | |