Die Konfiguration der externen FPolicy Engine planen

ONTAP 9

NetApp
September 23, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nas-audit/plan-fpolicy-external-engine-config-concept.html on September 23, 2026. Always check docs.netapp.com for the latest.

Inhalt

Die Konfiguration der externen FPolicy Engine planen . . . 1
Informationen zur Konfiguration der externen Engine von ONTAP FPolicy . . . 1
Informationen, die beim Erstellen der externen FPolicy Engine definiert werden . . . 1
Was die grundlegenden externen Engine-Parameter sind . . . 2
Was die erweiterten externen Engine-Optionen sind . . . 5
Wie externe ONTAP FPolicy-Engines SSL-authentifizierte Verbindungen verwenden . . . 7
SSL-Serverauthentifizierung . . . 8
Gegenseitige Authentifizierung . . . 8
Zertifikate für SSL installieren . . . 8
ONTAP FPolicy Zertifikatreplikation bei SVM Notfallwiederherstellung ohne ID-Erhaltung . . . 8
Einschränkungen für externe FPolicy-Engines mit MetroCluster und SVM-Notfallwiederherstellung in ONTAP . . . 9
ONTAP FPolicy Konfigurationsarbeitsblätter für externe Engines . . . 9
Informationen für eine grundlegende externe Engine-Konfiguration . . . 9
Informationen zu erweiterten externen Engine-Parametern . . . 10

Die Konfiguration der externen FPolicy Engine planen

Informationen zur Konfiguration der externen Engine von ONTAP FPolicy

Bevor Sie die externe FPolicy Engine konfigurieren, ist es wichtig zu verstehen, was die Erstellung einer externen Engine bedeutet und welche Konfigurationsparameter verfügbar sind. Diese Informationen unterstützen dabei, die passenden Werte für jeden Parameter festzulegen.

Informationen, die beim Erstellen der externen FPolicy Engine definiert werden

Die externe Engine-Konfiguration definiert die Informationen, die FPolicy benötigt, um Verbindungen zu den externen FPolicy-Servern herzustellen und zu verwalten, einschließlich der folgenden:

- SVM-Name
- Name der Engine
- Die IP-Adressen der primären und sekundären FPolicy Server sowie die TCP-Portnummer, die für die Verbindung zu den FPolicy Servern verwendet wird
- Ob der Engine-Typ asynchron oder synchron ist
- Ob das Engine-Format `xml` oder `protobuf` ist

  Ab ONTAP 9.15.1 kann das `protobuf` Engine-Format verwendet werden. Wenn auf `protobuf` gesetzt, werden die Benachrichtigungsnachrichten binär mit Google Protobuf codiert. Bevor das Engine-Format auf `protobuf` gesetzt wird, ist sicherzustellen, dass der FPolicy Server auch `protobuf` Deserialisierung unterstützt.

  Da das Protobuf-Format ab ONTAP 9.15.1 unterstützt wird, ist das externe Engine-Format zu berücksichtigen, bevor auf eine frühere Version von ONTAP zurückgegangen wird. Bei einer Rückkehr zu einer früheren Version als ONTAP 9.15.1 ist gemeinsam mit dem FPolicy Partner eine der folgenden Optionen zu prüfen:

  - Jedes Engine-Format wird von `protobuf` zu `xml` geändert
  - Die Engines mit einem Engine-Format von `protobuf` löschen
- Authentifizierung der Verbindung zwischen dem Knoten und dem FPolicy Server

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

- Verwaltung der Verbindung mit verschiedenen erweiterten Berechtigungseinstellungen

  Dies umfasst Parameter, die Dinge wie Zeitüberschreitungswerte, Retry-Werte, Keep-Alive-Werte, maximale Anforderungswerte, Werte für die Größe des Sende- und Empfangspuffers sowie Sitzungs-Zeitüberschreitungswerte definieren.

Der `vserver fpolicy policy external-engine create`Befehl wird verwendet, um eine externe FPolicy Engine zu erstellen.

Was die grundlegenden externen Engine-Parameter sind

Die folgende Tabelle mit grundlegenden FPolicy Konfigurationsparametern kann bei der Planung Ihrer Konfiguration unterstützen:

Art der Information	Option
SVM Gibt den SVM-Namen an, der mit dieser externen Engine verknüpft werden soll. Jede FPolicy Konfiguration ist innerhalb einer einzelnen SVM definiert. Die externe Engine, das Richtlinienereignis, der Richtlinienbereich und die Richtlinie, die zusammen eine FPolicy Richtlinienkonfiguration bilden, müssen alle derselben SVM zugeordnet sein.	`-vserver vserver_name`
Engine-Name Gibt den Namen an, der der externen Engine Konfiguration zugewiesen werden soll. Der Name der externen Engine muss später beim Erstellen der FPolicy Policy angegeben werden. Dadurch wird die externe Engine mit der Policy verknüpft. Der Name darf maximal 256 Zeichen lang sein. ⓘ Der Name sollte maximal 200 Zeichen lang sein, wenn der Name der externen Engine in einer MetroCluster oder SVM-Disaster-Recovery-Konfiguration konfiguriert wird. Der Name kann jede beliebige Kombination der folgenden ASCII-Zeichen enthalten: • `a`durch `z` • `A`durch `Z` • `0`durch `9` • “_”, “-”, and “.”	`-engine-name engine_name`

Primäre FPolicy Server Gibt die primären FPolicy Server an, an die der Knoten Benachrichtigungen für eine bestimmte FPolicy Richtlinie sendet. Der Wert wird als durch Kommas getrennte Liste von IP-Adressen angegeben. Wenn mehr als eine primäre Server-IP-Adresse angegeben ist, stellt jeder Knoten, an dem die SVM beteiligt ist, zum Zeitpunkt der Aktivierung der Richtlinie eine Steuerverbindung zu jedem angegebenen primären FPolicy Server her. Wenn mehrere primäre FPolicy Server konfiguriert werden, werden Benachrichtigungen im Round-Robin-Verfahren an die FPolicy Server gesendet. Wenn die externe Engine in einer MetroCluster oder SVM-Disaster-Recovery-Konfiguration verwendet wird, sollten die IP-Adressen der FPolicy-Server am Quellstandort als primäre Server angegeben werden. Die IP-Adressen der FPolicy-Server am Zielstandort sollten als sekundäre Server angegeben werden.	`-primary-servers IP_address,...`
Portnummer Gibt die Portnummer des FPolicy Dienstes an.	`-port integer`
Sekundäre FPolicy Server Gibt die sekundären FPolicy-Server an, an die die Dateizugriffsereignisse für eine bestimmte FPolicy-Richtlinie gesendet werden. Der Wert wird als durch Kommas getrennte Liste von IP-Adressen angegeben. Sekundäre Server werden nur verwendet, wenn keiner der primären Server erreichbar ist. Verbindungen zu sekundären Servern werden hergestellt, wenn die Richtlinie aktiviert ist, aber Benachrichtigungen werden nur an sekundäre Server gesendet, wenn keiner der primären Server erreichbar ist. Wenn mehrere sekundäre Server konfiguriert sind, werden Benachrichtigungen im Round-Robin-Verfahren an die FPolicy Server gesendet.	`-secondary-servers IP_address,...`
Externer Engine-Typ Legt fest, ob die externe Engine im synchronen oder asynchronen Modus arbeitet. Standardmäßig arbeitet FPolicy im synchronen Modus. Wenn auf `synchronous` gesetzt, sendet die Dateianforderungsverarbeitung eine Benachrichtigung an den FPolicy Server, wird jedoch erst nach Erhalt einer Antwort vom FPolicy Server fortgesetzt. Zu diesem Zeitpunkt wird der Anforderungsfluss entweder fortgesetzt oder die Verarbeitung führt zu einer Ablehnung, abhängig davon, ob die Antwort des FPolicy Servers die angeforderte Aktion zulässt. Wenn auf `asynchronous` gesetzt, sendet die Dateianforderungsverarbeitung 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 sein: • `synchronous` • `asynchronous`

Externes Engine Format Geben Sie an, ob das externe Engine-Format xml oder protobuf ist. Ab ONTAP 9.15.1 kann das Protobuf-Engine-Format verwendet werden. Wenn protobuf ausgewählt ist, werden die Benachrichtigungsnachrichten in binärer Form mit Google Protobuf codiert. Vor dem Einstellen des Engine-Formats auf Protobuf ist sicherzustellen, dass der FPolicy Server ebenfalls die Protobuf-Deserialisierung unterstützt.	`- extern-engine-format` {`protobuf` oder `xml`}
SSL-Option für die Kommunikation mit dem FPolicy Server Legt die SSL-Option für die Kommunikation mit dem FPolicy Server fest. Dies ist ein Pflichtparameter. Eine der Optionen kann anhand der folgenden Informationen ausgewählt werden: • Wenn auf `no-auth` gesetzt, findet keine Authentifizierung statt. Die Kommunikationsverbindung wird über TCP hergestellt. • Wenn diese Option auf `server-auth` gesetzt ist, authentifiziert die SVM den FPolicy Server mittels SSL-Authentifizierung. • Wenn auf `mutual-auth` gesetzt, findet eine gegenseitige Authentifizierung zwischen der SVM und dem FPolicy Server statt; die SVM authentifiziert den FPolicy Server und der FPolicy Server authentifiziert die SVM. Wenn Sie die gegenseitige SSL-Authentifizierung konfigurieren, müssen Sie auch die `-certificate-common-name`, `-certificate -serial` und `-certifcate-ca` Parameter konfigurieren.	`-ssl-option` {`no-auth`
`server-auth`	`mutual-auth`}
FQDN des Zertifikats oder benutzerdefinierter allgemeiner Name Gibt den Zertifikatsnamen an, der verwendet wird, wenn die SSL-Authentifizierung zwischen der SVM und dem FPolicy Server konfiguriert ist. Der Zertifikatsname kann als FQDN oder als benutzerdefinierter allgemeiner Name angegeben werden. Wenn Sie `mutual-auth` für den `-ssl-option` Parameter angeben, muss ein Wert für den `-certificate-common-name` Parameter angegeben werden.	`-certificate-common -name` `text`
Seriennummer des Zertifikats Gibt die Seriennummer des Zertifikats an, das für die Authentifizierung verwendet wird, wenn eine SSL-Authentifizierung zwischen der SVM und dem FPolicy Server konfiguriert ist. Wenn Sie `mutual-auth` für den `-ssl-option` Parameter angeben, muss ein Wert für den `-certificate-serial` Parameter angegeben werden.	`-certificate-serial` `text`

Zertifizierungsstelle Gibt den CA-Namen des Zertifikats an, das für die Authentifizierung verwendet wird, wenn eine SSL-Authentifizierung zwischen der SVM und dem FPolicy Server konfiguriert ist. Wenn Sie `mutual-auth` für den `-ssl-option` Parameter angeben, muss ein Wert für den `-certificate-ca` Parameter angegeben werden.	`-certificate-ca text`

Was die erweiterten externen Engine-Optionen sind

Die folgende Tabelle mit erweiterten FPolicy-Konfigurationsparametern bietet eine Übersicht, um zu entscheiden, ob die Konfiguration mit erweiterten Parametern angepasst werden soll. Diese Parameter dienen zur Anpassung des Kommunikationsverhaltens zwischen den Cluster-Knoten und den FPolicy Servern:

Art der Information	Option
Zeitüberschreitung beim Abbrechen einer Anfrage Gibt das Zeitintervall in Stunden (`h`), Minuten (`m`) oder Sekunden (`s`) an, das der Knoten auf eine Antwort vom FPolicy Server wartet. Läuft das Zeitüberschreitungsintervall ab, sendet der Knoten eine Abbruchanfrage an den FPolicy Server. Anschließend sendet der Knoten die Benachrichtigung an einen alternativen FPolicy Server. Diese Zeitüberschreitung hilft bei der Behandlung eines nicht reagierenden FPolicy Servers, was die Antwortzeiten von SMB/NFS-Clients verbessern kann. Auch das Abbrechen von Anfragen nach einer Zeitüberschreitung kann zur Freigabe von Systemressourcen beitragen, da die Benachrichtigungsanfrage von einem ausgefallenen oder fehlerhaften FPolicy Server an einen alternativen FPolicy Server verschoben wird. Der Wertebereich für diesen Wert ist `0` bis `100`. Wenn der Wert auf `0` gesetzt ist, ist die Option deaktiviert und Abbruchanforderungen werden nicht an den FPolicy Server gesendet. Der Standardwert ist `20s`.	`-reqs-cancel-timeout integer`[h
m	s]
Zeitüberschreitung beim Abbruch einer Anfrage Gibt die Zeitüberschreitung in Stunden (`h`), Minuten (`m`) oder Sekunden (`s`) für den Abbruch einer Anfrage an. Der Wertebereich für diesen Wert ist `0` bis `200`.	`-reqs-abort-timeout ` `integer`[h
m	s]
Intervall für das Senden von Statusanfragen Gibt das Intervall in Stunden (`h`), Minuten (`m`) oder Sekunden (`s`) an, nach dem eine Statusanfrage an den FPolicy Server gesendet wird. Der Wertebereich für diesen Wert ist `0` bis `50`. Wenn der Wert auf `0` gesetzt ist, ist die Option deaktiviert und Statusanforderungsmeldungen werden nicht an den FPolicy Server gesendet. Der Standardwert ist `10s`.	`-status-req-interval integer`[h

m	s]
Maximale Anzahl ausstehender Anfragen auf dem FPolicy Server Gibt die maximale Anzahl ausstehender Anfragen an, die auf dem FPolicy Server in die Warteschlange gestellt werden können. Der Wertebereich für diesen Wert ist `1` bis `10000`. Der Standardwert ist `500`.	`-max-server-reqs integer`
Zeitüberschreitung beim Trennen der Verbindung zu einem nicht reagierenden FPolicy Server Gibt das Zeitintervall in Stunden (`h`), Minuten (`m`) oder Sekunden (`s`) an, nach dem die Verbindung zum FPolicy Server beendet wird. Die Verbindung wird nach Ablauf der Zeitüberschreitungsperiode nur dann getrennt, wenn die Warteschlange des FPolicy-Servers die maximal zulässige Anzahl an Anfragen enthält und innerhalb der Zeitüberschreitungsperiode keine Antwort empfangen wird. Die maximal zulässige Anzahl an Anfragen ist entweder `50` (der Standardwert) oder die durch den `max-server-reqs-` Parameter festgelegte Anzahl. Der Wertebereich für diesen Wert ist `1` bis `100`. Der Standardwert ist `60s`.	`-server-progress -timeout integer`[h
m	s]
Intervall für das Senden von Keep-Alive-Nachrichten an den FPolicy Server Gibt das Zeitintervall in Stunden (`h`), Minuten (`m`) oder Sekunden (`s`) an, in dem Keep-Alive-Nachrichten an den FPolicy Server gesendet werden. Keep-alive-Nachrichten erkennen halbgeöffnete Verbindungen. Der Wertebereich für diesen Wert ist `10` bis `600`. Wenn der Wert auf `0` gesetzt ist, ist die Option deaktiviert und Keep-Alive-Nachrichten werden nicht an die FPolicy Server gesendet. Der Standardwert ist `120s`.	`-keep-alive-interval- integer`[h
m	s]
Maximale Anzahl an Wiederverbindungsversuchen Legt die maximale Anzahl der Versuche fest, die die SVM unternimmt, um die Verbindung zum FPolicy Server wiederherzustellen, nachdem die Verbindung unterbrochen wurde. Der Wertebereich für diesen Wert ist `0` bis `20`. Der Standardwert ist `5`.	`-max-connection-retries integer`

Empfangspuffergröße Legt die Empfangspuffergröße des verbundenen Sockets für den FPolicy Server fest. Der Standardwert ist auf 256 Kilobyte (Kb) eingestellt. Wenn der Wert auf 0 gesetzt ist, wird die Größe des Empfangspuffers auf einen vom System definierten Wert festgelegt. Wenn beispielsweise die Standardgröße des Empfangspuffers des Sockets 65536 Byte beträgt, wird durch Setzen des einstellbaren Werts auf 0 die Socket-Puffergröße auf 65536 Byte festgelegt. Jeder Wert ungleich dem Standardwert kann verwendet werden, um die Größe (in Byte) des Empfangspuffers festzulegen.	`-recv-buffer-size integer`
Sendepuffergröße Legt die Größe des Sendepuffers des verbundenen Sockets für den FPolicy Server fest. Der Standardwert ist auf 256 Kilobyte (Kb) eingestellt. Wenn der Wert auf 0 gesetzt ist, wird die Größe des Sendepuffers auf einen vom System definierten Wert festgelegt. Wenn beispielsweise die Standardgröße des Sendepuffers des Sockets auf 65536 Byte festgelegt ist, wird durch Setzen des anpassbaren Werts auf 0 die Socket-Puffergröße auf 65536 Byte eingestellt. Jeder Wert ungleich dem Standardwert kann verwendet werden, um die Größe (in Byte) des Sendepuffers festzulegen.	`-send-buffer-size integer`
Zeitüberschreitung beim Löschen einer Sitzungs-ID während der Wiederverbindung Gibt das Intervall in Stunden (`h`), Minuten (`m`) oder Sekunden (`s`) an, nach dem bei Wiederverbindungsversuchen eine neue Sitzungs-ID an den FPolicy Server gesendet wird. Wird die Verbindung zwischen dem Storage Controller und dem FPolicy Server unterbrochen und innerhalb des `-session-timeout` Intervalls wiederhergestellt, wird die alte Sitzungs-ID an den FPolicy Server gesendet, damit dieser Antworten auf alte Benachrichtigungen senden kann. Der Standardwert ist auf 10 Sekunden eingestellt.	`-session-timeout [integerh][integerm][integers]`

Wie externe ONTAP FPolicy-Engines SSL-authentifizierte Verbindungen verwenden

Einige zusätzliche Informationen sind erforderlich, wenn die externe FPolicy Engine für die Verwendung von SSL bei der Verbindung mit FPolicy Servern konfiguriert werden soll.

SSL-Serverauthentifizierung

Wenn Sie die externe FPolicy Engine für die SSL-Serverauthentifizierung konfigurieren, muss vor der Erstellung der externen Engine das öffentliche Zertifikat der Zertifizierungsstelle (CA), die das FPolicy Serverzertifikat signiert hat, installiert werden.

Gegenseitige Authentifizierung

Wenn externe FPolicy Engines so konfiguriert werden, dass sie bei der Verbindung von Storage Virtual Machine (SVM) Daten-LIFs mit externen FPolicy Servern die gegenseitige SSL Authentifizierung verwenden, muss vor der Erstellung der externen Engine das öffentliche Zertifikat der CA, die das FPolicy Serverzertifikat signiert hat, zusammen mit dem öffentlichen Zertifikat und der Schlüsseldatei für die Authentifizierung der SVM installiert werden. Dieses Zertifikat darf nicht gelöscht werden, solange FPolicy Richtlinien das installierte Zertifikat verwenden.

Wird das Zertifikat gelöscht, während FPolicy es für die gegenseitige Authentifizierung bei der Verbindung zu einem externen FPolicy Server verwendet, kann eine deaktivierte FPolicy Richtlinie, die dieses Zertifikat nutzt, nicht wieder aktiviert werden. Die FPolicy Richtlinie kann in diesem Fall auch dann nicht reaktiviert werden, wenn ein neues Zertifikat mit denselben Einstellungen erstellt und auf der SVM installiert wird.

Wenn das Zertifikat gelöscht wurde, ist ein neues Zertifikat zu installieren, neue FPolicy externe Engines zu erstellen, die das neue Zertifikat verwenden, und die neuen externen Engines der FPolicy Richtlinie zuzuordnen, die durch Ändern der FPolicy Richtlinie wieder aktiviert werden soll.

Zertifikate für SSL installieren

Das öffentliche Zertifikat der Zertifizierungsstelle, das zum Signieren des FPolicy Serverzertifikats verwendet wird, wird mit dem `security certificate install` Befehl und dem `-type` Parameter, der auf `client-ca` gesetzt ist, installiert. Der für die Authentifizierung der SVM erforderliche private Schlüssel und das öffentliche Zertifikat werden mit dem `security certificate install` Befehl und dem `-type` Parameter, der auf `server` gesetzt ist, installiert.

Verwandte Informationen

- "Sicherheitszertifikat installieren"

ONTAP FPolicy Zertifikatreplikation bei SVM Notfallwiederherstellung ohne ID-Erhaltung

Die für die SSL-Authentifizierung bei Verbindungen zu FPolicy Servern verwendeten Sicherheitszertifikate werden nicht auf SVM Disaster Recovery-Ziele mit Konfigurationen ohne ID-Erhaltung repliziert. Obwohl die FPolicy External-Engine-Konfiguration auf der SVM repliziert wird, werden die Sicherheitszertifikate nicht repliziert. Die Sicherheitszertifikate müssen manuell auf dem Ziel installiert werden.

Wenn Sie die SVM-Notfallwiederherstellungsbeziehung einrichten, bestimmt der Wert, den Sie für die `-identity-preserve` Option des `snapmirror create` Befehls auswählen, die Konfigurationsdetails, die in die Ziel-SVM repliziert werden.

Wenn die `-identity-preserve` Option auf `true` (ID-preserve) gesetzt ist, werden alle FPolicy-Konfigurationsdetails einschließlich der Informationen zum Sicherheitszertifikat repliziert. Die Sicherheitszertifikate müssen nur auf dem Ziel installiert werden, wenn die Option auf `false` (non-ID-

preserve) gesetzt ist.

Verwandte Informationen

- "snapmirror create"

Einschränkungen für externe FPolicy-Engines mit MetroCluster und SVM-Notfallwiederherstellung in ONTAP

Sie können eine clusterweite externe FPolicy-Engine erstellen, indem Sie die Cluster-Speicher-VM (SVM) der externen Engine zuweisen. Bei der Erstellung einer clusterweiten externen Engine in einer MetroCluster oder SVM-Disaster-Recovery-Konfiguration bestehen jedoch bestimmte Einschränkungen bei der Auswahl des Authentifizierungsverfahrens, das die SVM für die externe Kommunikation mit dem FPolicy-Server verwendet.

Es stehen drei Authentifizierungsoptionen zur Auswahl, wenn externe FPolicy-Server erstellt werden: keine Authentifizierung, SSL-Serverauthentifizierung und SSL-Gegenseitige Authentifizierung. Obwohl bei der Auswahl der Authentifizierungsoption keine Einschränkungen bestehen, wenn der externe FPolicy-Server einer Daten-SVM zugewiesen ist, gibt es Einschränkungen beim Erstellen einer FPolicy-Engine mit Cluster-Umfang:

Konfiguration	Gestattet?
MetroCluster oder SVM-Notfallwiederherstellung und eine clusterweite externe FPolicy Engine ohne Authentifizierung (SSL ist nicht konfiguriert)	Ja
MetroCluster oder SVM-Notfallwiederherstellung und eine clusterweite externe FPolicy Engine mit SSL-Server oder gegenseitiger SSL-Authentifizierung	Nein

- Wenn eine FPolicy-Engine mit Cluster-Bezug und externer Engine sowie SSL-Authentifizierung vorhanden ist und eine MetroCluster oder SVM Disaster Recovery-Konfiguration erstellt werden soll, muss diese externe Engine so geändert werden, dass keine Authentifizierung verwendet wird, oder die externe Engine muss entfernt werden, bevor die MetroCluster oder SVM Disaster Recovery-Konfiguration erstellt werden kann.
- Wenn die MetroCluster oder SVM-Notfallwiederherstellungskonfiguration bereits existiert, verhindert ONTAP die Erstellung einer clusterweiten FPolicy externen Engine mit SSL-Authentifizierung.

ONTAP FPolicy Konfigurationsarbeitsblätter für externe Engines

Sie können dieses Arbeitsblatt verwenden, um die Werte zu erfassen, die Sie während des FPolicy External Engine Konfigurationsprozesses benötigen. Falls ein Parameterwert erforderlich ist, sollte vor der Konfiguration der External Engine festgelegt werden, welcher Wert für diese Parameter zu verwenden ist.

Informationen für eine grundlegende externe Engine-Konfiguration

Es empfiehlt sich, festzuhalten, ob jede Parametereinstellung in die externe Engine Konfiguration aufgenommen werden soll, und anschließend den Wert der Parameter zu notieren, die aufgenommen werden

sollen.

Art der Information	Erforderlich	Enthalten	Ihre Werte
Name der Storage Virtual Machine (SVM)	Ja	Ja	
Name der Engine	Ja	Ja	
Primäre FPolicy Server	Ja	Ja	
Portnummer	Ja	Ja	
Sekundäre FPolicy Server	Nein		
Externer Engine-Typ	Nein		
SSL Option für die Kommunikation mit dem externen FPolicy Server	Ja	Ja	
Zertifikat FQDN oder benutzerdefinierter allgemeiner Name	Nein		
Zertifikatsseriennummer	Nein		
Zertifizierungsstelle	Nein		

Informationen zu erweiterten externen Engine-Parametern

Um eine externe Engine mit erweiterten Parametern zu konfigurieren, ist der Konfigurationsbefehl im erweiterten Berechtigungsmodus einzugeben.

Art der Information	Erforderlich	Enthalten	Ihre Werte
Zeitüberschreitung beim Abbrechen einer Anfrage	Nein		
Zeitüberschreitung beim Abbruch einer Anfrage	Nein		
Intervall für das Senden von Statusanfragen	Nein		
Maximale Anzahl ausstehender Anfragen auf dem FPolicy Server	Nein		
Zeitüberschreitung beim Trennen der Verbindung zu einem nicht reagierenden FPolicy Server	Nein		
Intervall für das Senden von Keep-Alive-Nachrichten an den FPolicy Server	Nein		
Maximale Anzahl an Wiederverbindungsversuchen	Nein		
Empfangspuffergröße	Nein		
Sendepuffergröße	Nein		
Zeitüberschreitung beim Löschen einer Sitzungs-ID während der Wiederverbindung	Nein		

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.