FPolicy外部エンジンの設定を計画する

ONTAP 9

NetApp
December 20, 2024

目次

FPolicy外部エンジンの設定を計画する

FPolicy外部エンジンの設定を計画する

FPolicy外部エンジンを設定する前に、外部エンジンを作成することの意味と、使用可能な設定パラメータを理解する必要があります。この情報は、各パラメータに設定する値を決定するのに役立ちます。

FPolicy外部エンジンの作成時に定義される情報

外部エンジンの設定では、外部FPolicyサーバへの接続を作成および管理するためにFPolicyが必要とする次のような情報を定義します。

- SVM名
- エンジン名
- FPolicyサーバへの接続時に使用するプライマリおよびセカンダリFPolicyサーバのIPアドレスとTCPポート番号
- エンジンタイプが非同期か同期か
- エンジンフォーマットがまたは `protobuf`かどうか `xml`

  ONTAP 9 .15.1以降では、エンジン形式を使用できます `protobuf`。に設定する `protobuf`と、通知メッセージはGoogle Protobufを使用してバイナリ形式でエンコードされます。エンジン形式をに設定する前に、 `protobuf`FPolicyサーバでもデシリアライゼーションがサポートされていることを確認して `protobuf`ください。

  protobuf形式はONTAP 9 .15.1以降でサポートされているため、以前のリリースのONTAPにリバートする前に外部エンジン形式を考慮する必要があります。ONTAP 9.15.1より前のリリースにリバートする場合は、FPolicyパートナーと協力して次のいずれかを実行します。

  - 各エンジンフォーマットをからに `xml`変更します。 `protobuf`
  - エンジンフォーマットがのエンジンを削除します。 `protobuf`
- ノードとFPolicyサーバ間の接続を認証する方法

  相互SSL認証を設定する場合は、SSL証明書情報を提供するパラメータも設定する必要があります。
- 各種の高度な権限設定を使用して接続を管理する方法

  これには、タイムアウト値、リトライ値、キープアライブ値、最大要求値、送信および受信バッファ サイズ値、セッション タイムアウト値などを定義するパラメータが含まれます。

コマンドは、 `vserver fpolicy policy external-engine create`FPolicy外部エンジンの作成に使用します。

外部エンジンの基本パラメータ

次に示すFPolicy基本設定パラメータの一覧は、設定を計画するのに役立ちます。

情報の種類	オプション
SVM この外部エンジンに関連付けるSVMの名前を指定します。 各FPolicy設定は、単一のSVM内で定義されます。FPolicyポリシーの構成要素となる外部エンジン、ポリシーイベント、ポリシーのスコープ、およびポリシーを、すべて同じSVMに関連付ける必要があります。	`-vserver vserver_name`
_ エンジン名 _ 外部エンジンの設定に割り当てる名前を指定します。FPolicyポリシーを作成した場合、あとで外部エンジンの名前を指定する必要があります。こうすることで、外部エンジンがポリシーに関連付けられます。 名前の最大文字数は256文字です。 MetroClusterまたはSVMディザスタリカバリ設定で外部エンジン名を設定する場合、この名前は最大200文字にする必要があります。 名前には、次のASCII文字の任意の組み合わせを含めることができます。 • a`から `z • A`から `Z • 0`から `9 • “_”、“.”-", and "	`-engine-name engine_name`
プライマリ FPolicy サーバ _ 所定のFPolicyポリシーに関してノードが送信する通知の宛先となるプライマリFPolicyサーバを指定します。IPアドレスの値をカンマで区切って指定します。 複数のプライマリサーバのIPアドレスを指定した場合、SVMが参加しているすべてのノードに、ポリシーが有効になったときに指定されたすべてのプライマリFPolicyサーバへの制御接続が作成されます。複数のプライマリFPolicyサーバを設定した場合、通知はラウンドロビン方式でFPolicyサーバに送信されます。 外部エンジンがMetroClusterまたはSVMディザスタリカバリ設定で使用されている場合は、ソースサイトでのFPolicyサーバのIPアドレスをプライマリサーバとして指定する必要があります。デスティネーションサイトのFPolicyサーバのIPアドレスは、セカンダリサーバとして指定する必要があります。	`-primary-servers IP_address`はい。

ポート番号 _ FPolicyサービスのポート番号を指定します。	`-port integer`
_ セカンダリ FPolicy サーバ _ 所定のFPolicyポリシーに関して、ファイルアクセスイベントの送信先となるセカンダリFPolicyサーバを指定します。IPアドレスの値をカンマで区切って指定します。 セカンダリサーバは、いずれのプライマリサーバにも到達できない場合にのみ使用されます。ポリシーを有効にすると、セカンダリサーバへの接続が確立されますが、通知がセカンダリサーバに送信されるのは、いずれのプライマリサーバにも到達できない場合だけです。複数のセカンダリサーバを設定した場合、通知はラウンドロビン方式でFPolicyサーバに送信されます。	`-secondary-servers` `IP_address`はい。
_ 外部エンジンタイプ _ 外部エンジンが同期モードで動作するか非同期モードで動作するかを指定します。デフォルトでは、FPolicyは同期モードで動作します。 に設定する `synchronous`と、ファイル要求処理によって通知がFPolicyサーバに送信されますが、その後FPolicyサーバから応答を受信するまでは通知は送信されません。この時点で、要求されたアクションがFPolicyサーバからの応答で許可されるかどうかに応じて、要求フローが続行されるか処理が拒否されます。 に設定する `asynchronous`と、ファイル要求処理はFPolicyサーバに通知を送信したあとも続行します。	`-extern-engine-type` `external_engine_type`このパラメータには、次のいずれかの値を指定できます。 • `synchronous` • `asynchronous`
外部エンジンフォーマット 外部エンジン形式がXMLかprotobufかを指定します。 ONTAP 9 .15.1以降では、protobufエンジン形式を使用できます。protobufに設定すると、通知メッセージはGoogle Protobufを使用してバイナリ形式でエンコードされます。エンジン形式をprotobufに設定する前に、FPolicyサーバでもprotobufデシリアライゼーションがサポートされていることを確認してください。	`- extern-engine-format` {`protobuf` または `xml`}

_SSL オプションを使用して FPolicy サーバと通信します FPolicyサーバとの通信に使用するSSLオプションを指定します。これは必須パラメータです。次の情報に基づいて、いずれかのオプションを選択できます。 • に設定する `no-auth`と、認証は行われません。 通信リンクはTCPを介して確立されます。 • に設定する `server-auth`と、SVMはSSLサーバ認証を使用してFPolicyサーバを認証します。 • に設定する `mutual-auth`と、SVMとFPolicyサーバの間で相互認証が行われ、SVMはFPolicyサーバを認証し、FPolicyサーバはSVMを認証します。 相互SSL認証を設定する場合は、、 `-certificate-serial`、の `-certifcate-ca`各パラメータも設定する必要があります `-certificate-common-name`。	`-ssl-option{no-auth`
`server-auth`	`mutual-auth}`
_ 証明書 FQDN またはカスタム共通名 _ SVMとFPolicyサーバ間のSSL認証が設定されている場合に使用される証明書の名前を指定します。証明書の名前は、FQDNまたはカスタム共通名で指定できます。 パラメータに `-ssl-option`を指定する場合 `mutual-auth`は、パラメータの値を指定する必要があります `-certificate-common-name`。	`-certificate-common-name text`
証明書シリアル番号 _ SVMとFPolicyサーバ間のSSL認証が設定されている場合に認証に使用される証明書のシリアル番号を指定します。 パラメータに `-ssl-option`を指定する場合 `mutual-auth`は、パラメータの値を指定する必要があります `-certificate-serial`。	`-certificate-serial text`
_ 認証局 _ SVMとFPolicyサーバ間のSSL認証が設定されている場合に認証に使用される証明書のCA名を指定します。 パラメータに `-ssl-option`を指定する場合 `mutual-auth`は、パラメータの値を指定する必要があります `-certificate-ca`。	`-certificate-ca text`

外部エンジンの詳細オプションとは

次の高度なFPolicy設定パラメータの表は、高度なパラメータを使用して設定をカスタマイズするかどうかを計画する際に使用できます。これらのパラメータを使用して、クラスタノードとFPolicyサーバ間の通信動作を変更します。

情報の種類	オプション
_ リクエストをキャンセルするためのタイムアウト _ (s`ノードがFPolicyサーバからの応答を待機する時間間隔（時間(`h）、分(m、または秒）を指定します。 タイムアウト間隔が経過すると、ノードはFPolicyサーバにキャンセル要求を送信します。その後、ノードから代替FPolicyサーバに通知が送信されます。このタイムアウトは、応答していないFPolicyサーバを処理するのに役立ちます。これにより、SMB / NFSクライアントの応答を改善できます。また、通知要求が停止している、または無効なFPolicyサーバから代替FPolicyサーバに移動されるため、タイムアウト時間後に要求をキャンセルすると、システムリソースを解放するのに役立ちます。 この値の範囲は~ 100`です `0。値がに設定されている場合 0、オプションは無効になり、キャンセル要求メッセージはFPolicyサーバに送信されません。デフォルトはです 20s。	-reqs-cancel-timeout integer[h
m	s]
_ 要求を破棄するためのタイムアウト _ (s`要求を中止するタイムアウト（時間）(`h、分(m、または秒）を指定します。 この値の範囲は~ 200`です `0。	-reqs-abort-timeout ` `integer[h
m	s]
ステータス要求の送信間隔 _ (s`FPolicyサーバにステータス要求を送信する間隔（時間(`h）、分）(m、または秒）を指定します。 この値の範囲は~ 50`です `0。値がに設定されている場合 0、オプションは無効になり、ステータス要求メッセージはFPolicyサーバに送信されません。デフォルトはです 10s。	-status-req-interval integer[h
m	s]
FPolicy サーバの未処理要求の最大数 _ FPolicyサーバのキューに登録できる未処理要求の最大数を指定します。 この値の範囲は~ 10000`です `1。デフォルトはです 500。	-max-server-reqs integer

_ 応答しない FPolicy サーバを切断するタイムアウト _ (s`FPolicyサーバへの接続を終了するまでの時間間隔（時間(`h）、分）(m、または秒を指定します。 FPolicyサーバのキューに許容される最大要求数が含まれていて、タイムアウト期間内に応答がない場合にのみ、タイムアウト期間後に接続を終了します。許可される最大要求数は、（デフォルト）またはパラメータで指定された数 max-server-reqs-`です `50。 この値の範囲は~ 100`です `1。デフォルトはです 60s。	-server-progress -timeout integer[h
m	s]
FPolicy サーバにキープアライブメッセージを送信する間隔 _ (s`FPolicyサーバにキープアライブメッセージを送信する時間間隔を時間(`h、分(m、または秒で指定します。 キープアライブメッセージはハーフオープン接続を検出します。 この値の範囲は~ 600`です `10。値がに設定されている場合 0、オプションは無効になり、キープアライブメッセージはFPolicyサーバに送信されません。デフォルトはです 120s。	-keep-alive-interval-integer[h
m	s]
最大再接続試行回数 _ 接続が切断されたあと、SVMがFPolicyサーバへの再接続を試行する最大回数を指定します。 この値の範囲は~ 20`です `0。デフォルトはです 5。	-max-connection-retries integer
受信バッファサイズ _ FPolicyサーバの接続ソケットの受信バッファサイズを指定します。 デフォルト値は256KBに設定されています。値が0に設定されている場合、受信バッファのサイズはシステムによって定義された値に設定されます。 たとえば、ソケットのデフォルトの受信バッファサイズが65536バイトの場合、調整可能な値を0に設定すると、ソケットバッファサイズは65536バイトに設定されます。デフォルト値以外の任意の値を使用して、受信バッファのサイズ（バイト単位）を設定できます。	-recv-buffer-size integer

送信バッファサイズ _ FPolicyサーバの接続ソケットの送信バッファサイズを指定します。 デフォルト値は256KBに設定されています。値が0に設定されている場合、送信バッファのサイズはシステムによって定義された値に設定されます。 たとえば、ソケットのデフォルトの送信バッファサイズが65536バイトに設定されている場合、調整可能な値を0に設定すると、ソケットバッファサイズは65536バイトに設定されます。デフォルト値以外の任意の値を使用して、送信バッファのサイズ（バイト単位）を設定できます。	`-send-buffer-size integer`
_ 再接続中にセッション ID を消去するためのタイムアウト _ (s`再接続の試行時にFPolicyサーバに新しいSession IDが送信されるまでの間隔（時間(`h）、分）(m、または秒を指定します。 ストレージコントローラとFPolicyサーバの間の接続が終了し、その期間内に再接続が行われる `-session-timeout`と、古い通知に対する応答を送信できるように、古いSession IDがFPolicyサーバに送信されます。 デフォルト値は10秒に設定されています。	`-session-timeout [h][m]integerintegerinteger`

SSL認証接続を使用するためのFPolicy外部エンジンの設定に関する詳細情報

FPolicyサーバへの接続時にSSLを使用するようにFPolicy外部エンジンを設定する場合は、いくつかの追加情報を確認しておく必要があります。

SSLサーバ認証

SSL サーバ認証用の FPolicy 外部エンジンを設定する場合には、外部エンジンを作成する前に、 FPolicy サーバ証明書の署名を行った認証局（ CA ）のパブリック証明書をインストールする必要があります。

相互認証

Storage Virtual Machine（SVM）のデータLIFを外部FPolicyサーバに接続するときにSSL相互認証を使用するようにFPolicy外部エンジンを設定する場合は、外部エンジンを作成する前に、FPolicyサーバ証明書の署名を行ったCAのパブリック証明書を、SVMの認証用のパブリック証明書およびキーファイルとともにインストールする必要があります。インストールされている証明書をFPolicyポリシーが使用している間は、この証明書を削除しないでください。

FPolicyが相互認証に証明書を使用しているときに証明書を削除した場合、その証明書を使用する無効になっているFPolicyポリシーを再度有効にすることはできません。この状況では、同じ設定で証明書を新規作成して SVM にインストールしても、 FPolicy ポリシーを再度有効にすることはできません。

証明書が削除されている場合は、新しい証明書をインストールし、その証明書を使用する新しいFPolicy外部エンジンを作成し、FPolicyポリシーを変更して再度有効にするFPolicyポリシーに新しい外部エンジンを関連付ける必要があります。

SSL用の証明書のインストール

FPolicyサーバ証明書に署名したCAのパブリック証明書をインストールするには、コマンドで `-type`パラメータをに設定 `client-ca`し `security certificate install`ます。SVMの認証に必要な秘密鍵とパブリック証明書をインストールするには、コマンドを `-type`使用して、 `security certificate install`パラメータをに設定 `server`します。

IDが保持されない設定のSVMディザスタリカバリ関係でレプリケートされない証明書

FPolicyサーバへの接続時にSSL認証に使用されるセキュリティ証明書は、IDが保持されない設定のSVMディザスタリカバリ先にレプリケートされません。SVM上のFPolicy外部エンジンの設定はレプリケートされますが、セキュリティ証明書はレプリケートされません。セキュリティ証明書をデスティネーションに手動でインストールする必要があります。

SVMディザスタリカバリ関係の設定時にコマンドのオプション `snapmirror create`に選択した値 `-identity-preserve`によって、デスティネーションSVMにレプリケートされる設定の詳細が決まります。

このオプションを（ID保持）に `true`設定する `-identity-preserve`と、セキュリティ証明書の情報を含むすべてのFPolicy設定の詳細がレプリケートされます。セキュリティ証明書をデスティネーションにインストールする必要があるのは、オプションを（ID保持なし）に設定した場合だけ `false`です。

MetroClusterおよびSVMディザスタリカバリ設定を使用するクラスタ対象FPolicy外部エンジンの制限事項

クラスタを対象としたFPolicy外部エンジンを作成するには、クラスタStorage Virtual Machine（SVM）をそのエンジンに割り当てます。ただし、MetroClusterまたはSVMディザスタリカバリ設定でクラスタ対象の外部エンジンを作成する場合は、SVMがFPolicyサーバとの外部通信に使用する認証方式を選択する際に一定の制限事項があります。

外部FPolicyサーバの作成時に選択できる認証オプションには、認証なし、SSLサーバ認証、およびSSL相互認証の3つがあります。外部FPolicyサーバがデータSVMに割り当てられている場合に認証オプションを選択する際の制限事項はありませんが、クラスタ対象のFPolicy外部エンジンを作成する際には制限事項があります。

構成	許可されるかどうか
MetroClusterまたはSVMディザスタリカバリと、認証を行わないクラスタ対象FPolicy外部エンジン（SSL未設定）	○
MetroClusterまたはSVMディザスタリカバリと、SSLサーバまたはSSL相互認証を備えたクラスタ対象FPolicy外部エンジン	いいえ

- SSL認証を使用するクラスタ対象FPolicy外部エンジンが存在し、MetroClusterまたはSVMディザスタリカバリ設定を作成する場合は、認証を使用しないようにこの外部エンジンを変更するか、MetroClusterまたはSVMディザスタリカバリ設定を作成する前に外部エンジンを削除する必要があります。

- MetroClusterまたはSVMディザスタリカバリ設定がすでに存在する場合、ONTAPにより、SSL認証を使用するクラスタ対象FPolicy外部エンジンの作成が阻止されます。

FPolicy外部エンジンの設定ワークシートに記入する

このワークシートを使用して、FPolicy外部エンジンの設定プロセス中に必要となる値を記録できます。パラメータ値が必須の場合は、外部エンジンを設定する前に、それらのパラメータに使用する値を決定する必要があります。

外部エンジンの基本設定に関する情報

外部エンジンの設定に各パラメータ設定を含めるかどうかを記録し、含めるパラメータの値を記録しておく必要があります。

情報の種類	必須	含める	自分の価値観
Storage Virtual Machine（SVM）名	○	○	
エンジン名	○	○	
フライマリFPolicyサアハ	○	○	
ポート番号	○	○	
セカンダリFPolicyサーバ	いいえ		
外部エンジンタイプ	いいえ		
外部FPolicyサーバとの通信のためのSSLオプション	○	○	
証明書のFQDNまたはカスタム共通名	いいえ		
証明書のシリアル番号	いいえ		
認証局	いいえ		

外部エンジンの詳細パラメータに関する情報

外部エンジンに高度なパラメータを設定するには、advanced権限モードで設定コマンドを入力する必要があります。

情報の種類	必須	含める	自分の価値観
タイムアウトによる要求のキャンセル	いいえ		

タイムアウトによる要求の破棄	いいえ		
ステータス要求の送信間隔	いいえ		
FPolicyサーバの未処理要求の最大数	いいえ		
応答しないFPolicyサーバを切断するタイムアウト	いいえ		
FPolicyサーバへのキープアライブメッセージの送信間隔	いいえ		
再接続の最大試行回数	いいえ		
受信バッファサイズ	いいえ		
送信バッファサイズ	いいえ		
再接続中にSession IDをパージするためのタイムアウト	いいえ		

著作権に関する情報

商標に関する情報