FPolicy の設定を計画

ONTAP 9

NetApp
April 24, 2024

目次

FPolicy の設定を計画

FPolicy を設定するための要件、考慮事項、およびベストプラクティス

SVMでFPolicyの設定を作成して設定する前に、FPolicyの設定に関する一定の要件、考慮事項、およびベストプラクティスについて確認しておく必要があります。

FPolicy機能は、コマンドラインインターフェイス（CLI）またはREST APIを使用して設定します。

FPolicy を設定するための要件

Storage Virtual Machine （ SVM ）で FPolicy を設定して有効にする前に、一定の要件について確認しておく必要があります。

- クラスタ内のすべてのノードで、 FPolicy がサポートされているバージョンの ONTAP が実行されている必要があります。
- ONTAP の標準の FPolicy エンジンを使用しない場合は、外部 FPolicy サーバ（ FPolicy サーバ）をインストールしておく必要があります。
- FPolicy ポリシーが有効になっている SVM のデータ LIF からアクセスできるサーバに、 FPolicy サーバがインストールされている必要があります。

  ONTAP 9.8以降では、ONTAP により、を追加して、アウトバウンドFPolicy接続用のクライアントLIFサービスを利用できます `data-fpolicy-client` サービス "LIFとサービスポリシーの詳細については、こちらをご覧ください"。

- FPolicy ポリシーの外部エンジンの設定で、 FPolicy サーバの IP アドレスがプライマリサーバまたはセカンダリサーバとして設定されている必要があります。
- FPolicy サーバで権限付きデータチャネルを使用してデータにアクセスする場合は、次の追加要件を満たす必要があります。
  - クラスタで SMB のライセンスが有効になっている必要があります。

    権限付きデータアクセスは SMB 接続を使用して実行されます。

  - 権限付きデータチャネルを使用してファイルにアクセスするためのユーザクレデンシャルが設定されている必要があります。
  - FPolicy サーバが FPolicy の設定で指定されたクレデンシャルで実行されている。
  - FPolicyサーバとの通信に使用されるすべてのデータLIFをで設定する必要があります `cifs` 許可されているプロトコルの1つとして指定します。

    これには、パススルーリード接続で使用される LIF も含まれます。

- ONTAP 9.14.1以降では、FPolicyで永続的ストアを設定して、SVM内の非同期（必須ではない）ポリシーのファイルアクセスイベントをキャプチャすることができます。永続的ストアを使用すると、クライアントI/O処理とFPolicy通知処理を分離して、クライアントのレイテンシを低減できます。同期（必須または必須でない）および非同期の必須構成はサポートされていません。

FPolicy を設定する際のベストプラクティスと推奨事項

Storage Virtual Machine（SVM）でFPolicyを設定する場合は、FPolicyの設定によって監視のパフォーマンスが向上し、要件を満たす結果が得られるようにするために、設定に関する一般的なベストプラクティスと推奨事項を理解してください。

パフォーマンス、サイジング、および設定に関する具体的なガイドラインについては、FPolicyパートナーアプリケーションを参照してください。

ポリシー設定

FPolicy外部エンジン、イベント、SVM用のスコープを設定することで、全体的なエクスペリエンスとセキュリティが向上する可能性があります。

- SVM用のFPolicy外部エンジンの設定：
  - セキュリティを強化するには、パフォーマンスコストがかかります。Secure Sockets Layer（SSL）通信を有効にすると、共有へのアクセスのパフォーマンスに影響します。
  - FPolicyサーバの通知処理の耐障害性と高可用性を確保するには、FPolicy外部エンジンに複数のFPolicyサーバを設定する必要があります。
- SVMのFPolicyイベントの設定

  ファイル操作の監視は、エクスペリエンス全体に影響します。たとえば、ストレージ側で不要なファイル操作をフィルタリングすると、操作性が向上します。NetAppでは、次の設定を推奨しています。

  - ユースケースを壊さずに、最小タイプのファイル処理を監視し、最大数のフィルタを有効にする。
  - 属性取得、読み取り、書き込み、オープン、クローズの各処理にフィルタを使用する。SMBおよびNFSホームディレクトリ環境では、これらの処理の割合が高くなっています。
- SVMのFPolicyスコープの設定

  ポリシーの範囲を、SVM全体ではなく、関連するストレージオブジェクト（共有、ボリューム、エクスポートなど）に制限します。NetAppでは、ディレクトリ拡張子の確認を推奨しています状況に応じて `is-file-extension-check-on-directories-enabled` パラメータはに設定されます `true`の場合、ディレクトリオブジェクトには、通常のファイルと同じ拡張子チェックが適用されます。

ネットワーク構成：

FPolicyサーバとコントローラの間のネットワーク接続のレイテンシを低くする必要があります。NetAppでは、プライベートネットワークを使用してFPolicyトラフィックをクライアントトラフィックから分離することを推奨しています。

また、レイテンシを最小限に抑え、広帯域接続を実現するために、外部FPolicyサーバ（FPolicyサーバ）を広帯域接続が可能なクラスタの近くに配置する必要があります。

> FPolicyトラフィック用のLIFがクライアントトラフィック用のLIFとは別のポートに設定されている場合、ポートの障害が原因でFPolicy LIFがもう一方のノードにフェイルオーバーすることがあります。その結果、ノードからFPolicyサーバに到達できなくなり、ノードでのファイル操作に関するFPolicy通知は失敗します。この問題を回避するには、ノード上の少なくとも1つのLIFからFPolicyサーバにアクセスして、そのノードで実行されるファイル操作のFPolicy要求を処理できることを確認します。

ハードウェア構成

FPolicyサーバは物理サーバと仮想サーバのどちらにも配置できます。FPolicyサーバが仮想環境にある場合は、仮想サーバに専用のリソース（CPU、ネットワーク、およびメモリ）を割り当てる必要があります。

SVM がクライアント要求に応答する際のレイテンシの原因となる可能性がある FPolicy サーバの過負荷状態を防ぐために、クラスタノードと FPolicy サーバの比率を最適化する必要があります。最適な比率は、FPolicyサーバが使用されているパートナーアプリケーションによって異なります。NetAppでは、パートナーと協力して適切な価値を判断することを推奨しています。

複数ポリシーの設定

ネイティブブロッキング用のFPolicyポリシーはシーケンス番号に関係なく最も優先され、意思決定変更ポリシーは他のポリシーよりも優先されます。ポリシーの優先度はユースケースによって異なります。NetAppは、パートナーと協力して適切な優先順位を決定することを推奨します。

サイズに関する考慮事項

FPolicyは、SMB処理とNFS処理のインライン監視を実行し、外部サーバに通知を送信し、外部エンジンの通信モード（同期または非同期）に応じて応答を待機します。このプロセスは、SMBとNFSのアクセスおよびCPUリソースのパフォーマンスに影響します。

NetAppでは、問題を軽減するために、FPolicyを有効にする前に、パートナーと協力して環境を評価し、サイジングすることを推奨しています。パフォーマンスは、ユーザ数、ユーザあたりの処理数やデータサイズなどのワークロード特性、ネットワークレイテンシ、障害やサーバの速度低下など、いくつかの要因によって影響を受けます。

パフォーマンスを監視

FPolicyは通知ベースのシステムです。通知は、処理およびONTAPへの応答を生成するために外部サーバに送信されます。このラウンドトリッププロセスにより、クライアントアクセスのレイテンシが増加します。

FPolicyサーバとONTAPのパフォーマンスカウンタを監視すると、解決策のボトルネックを特定し、解決策を最適化するために必要に応じてパラメータを調整できます。たとえば、FPolicyのレイテンシの増加は、SMBとNFSのアクセスレイテンシに連鎖的に影響します。そのため、ワークロード（SMBとNFS）とFPolicyの両方のレイテンシを監視する必要があります。また、ONTAPのQoSポリシーを使用して、FPolicyが有効になっているボリュームまたはSVMごとにワークロードを設定できます。

NetAppは、を実行することを推奨します `statistics show -object workload` コマンドを使用してワークロード統計を表示します。さらに、次のパラメータを監視する必要があります。

- 平均レイテンシ、読み取りレイテンシ、書き込みレイテンシ
- 処理の総数
- 読み取りカウンタと書き込みカウンタ

FPolicyサブシステムのパフォーマンスを監視するには、次のFPolicyカウンタを使用します。

> FPolicyに関連する統計を収集するには、診断モードにする必要があります。

手順

1. FPolicyカウンタを収集します。

a. `statistics start -object fpolicy -instance instance_name -sample-id ID`

b. `statistics start -object fpolicy_policy -instance instance_name -sample-id ID`

2. FPolicyカウンタを表示します。

a. `statistics show -object fpolicy –instance instance_name -sample-id ID`

b. `statistics show -object fpolicy_server –instance instance_name -sample-id ID`

。 `fpolicy` および `fpolicy_server` カウンタは、次の表で説明されている複数のパフォーマンスパラメータに関する情報を提供します。

カウンタ	説明
「**fpolicy**」カウンタ	aborted_requests
SVMで処理が中止されたスクリーニング要求の数	event_count
通知の原因となるイベントのリスト	max_request_latencyの略
最大スクリーン要求遅延	outstanding_requests
処理中のスクリーン要求の総数	processed_requests
SVMでfpolicy処理が実行されたスクリーニング要求の総数	request_latency_hist
画面要求のレイテンシのヒストグラム	requests_dispatched_rate
1秒あたりに送出されるスクリーン要求の数	requests_received_rate
1秒あたりに受信された画面要求の数	「**fpolicy_server**」カウンタ
max_request_latencyの略	画面要求の最大遅延
outstanding_requests	応答を待機している画面要求の総数
request_latency	画面要求の平均遅延
request_latency_hist	画面要求のレイテンシのヒストグラム
request_sent_rate	FPolicyサーバに送信された1秒あたりのスクリーニング要求数
response_received_rate	FPolicyサーバから受信した1秒あたりのスクリーニング応答数

FPolicyワークフローと他のテクノロジへの依存関係を管理します

NetAppでは、設定を変更する前にFPolicyポリシーを無効にすることを推奨しています。たとえば、有効なポリシーに設定されている外部エンジンのIPアドレスを追加または変更する場合は、最初にポリシーを無効にします。

NetApp FlexCacheボリュームを監視するようにFPolicyを設定する場合は、NetApp読み取りおよび属性取得ファイル操作を監視するようにFPolicyを設定しないことを推奨します。ONTAPでこれらの処理を監視するには、inode-to-path（I2P）データを取得する必要があります。I2PデータはFlexCacheボリュームから取得できないため、元のボリュームから取得する必要があります。そのため、これらの処理を監視することで、FlexCacheが提供するパフォーマンス上のメリットが排除されます。

FPolicyと外部のウィルス対策解決策の両方が導入されている場合、最初にウィルス対策解決策が通知を受信します。FPolicyの処理は、ウィルス対策スキャンの完了後に開始されます。低速のウィルス対策スキャナは全体的なパフォーマンスに影響する可能性があるため、ウィルス対策ソリューションのサイズを正しく設定することが重要です。

パススルーリードのアップグレードおよびリバートに関する考慮事項

パススルーリードをサポートしている ONTAP リリースへのアップグレードまたはパススルーリードをサポートしていないリリースへのリバートを行う前に、アップグレードおよびリバートに関する考慮事項を把握しておく必要があります。

をアップグレードして

FPolicy パススルーリードをサポートしている ONTAP のバージョンにすべてのノードをアップグレードしたあと、クラスタはパススルーリードを使用できるようになります。ただし、既存の FPolicy 設定ではパススルーリードがデフォルトで無効になっています。既存の FPolicy 設定でパススルーリードを使用するには、FPolicy ポリシーを無効にして設定を変更してから、設定を再度有効にする必要があります。

復元しています

FPolicyパススルーリードをサポートしていないバージョンのONTAPにリバートする前に、次の条件を満たす必要があります。

- パススルーリードを使用してすべてのポリシーを無効にし、パススルーリードを使用しないように影響を受ける設定を変更します。
- クラスタのすべてのFPolicyポリシーを無効にして、クラスタのFPolicy機能を無効にします。

永続的ストアをサポートしないバージョンのONTAPにリバートする前に、FPolicyポリシーに永続的ストアが設定されていないことを確認してください。永続ストアが設定されている場合、リバートは失敗します。

FPolicy の設定手順は何ですか

FPolicy でファイルアクセスを監視するには、 FPolicy の設定を作成し、 FPolicy サービスが必要な Storage Virtual Machine （ SVM ）で有効にする必要があります。

SVM で FPolicy 設定をセットアップして有効にする手順は次のとおりです。

1. FPolicy 外部エンジンを作成します。

   FPolicy 外部エンジンでは、特定の FPolicy の設定に関連付けられた外部 FPolicy サーバ（ FPolicy サーバ）を識別します。内部の「ネイティブ」 FPolicy エンジンを使用してネイティブ・ファイル・ブロッキング構成を作成する場合は、 FPolicy 外部エンジンを作成する必要はありません。

2. FPolicy イベントを作成します。

FPolicy イベントでは、 FPolicy ポリシーで監視する対象を定義します。監視対象のプロトコルとファイル操作を指定し、一連のフィルタを含めることができます。それらのフィルタを使用して、監視対象イベントの中から、 FPolicy 外部エンジンで通知を送信する必要があるイベントだけを抽出できます。イベントでは、ポリシーでボリューム操作を監視するかどうかも指定します。

3. FPolicy ポリシーを作成します。

   FPolicy ポリシーでは、監視する必要がある一連のイベントと、指定の FPolicy サーバ（ FPolicy サーバが設定されていない場合は標準のエンジン）に通知を送信する必要がある監視対象イベントを、適切な範囲で関連付けます。また、通知を受信するデータへの権限付きアクセスを FPolicy サーバに許可するかどうかも定義します。FPolicy サーバからデータにアクセスする必要がある場合は、権限付きアクセスが必要になります。権限付きアクセスが必要になる一般的なユースケースとしては、ファイルブロッキング、クォータ管理、階層型ストレージ管理などがあります。ポリシーは、このポリシーの設定で FPolicy サーバを使用するか、内部の「ネイティブ」 FPolicy サーバを使用するかを指定します。

   スクリーニングを必須にするかどうかはポリシーで指定します。スクリーニングを必須にすると、すべての FPolicy サーバが停止した場合や定義された時間内に FPolicy サーバからの応答を得られない場合に、ファイルアクセスが拒否されます。

   ポリシーは SVM 単位で適用されます。1 つのポリシーを複数の SVM に適用することはできません。ただし、 SVM には複数の FPolicy ポリシーを設定でき、各ポリシーのスコープ、イベント、外部サーバの設定を同じ組み合わせにすることも、それぞれで異なる組み合わせにすることもできます。

4. ポリシーのスコープを設定します。

   FPolicy スコープでは、ポリシーで監視するボリューム、共有、またはエクスポートポリシーを指定します。また、 FPolicy による監視対象に含めるファイル拡張子や除外するファイル拡張子も指定します。

   除外リストは、対象リストよりも優先されます。

5. FPolicy ポリシーを有効にします。

   ポリシーを有効にすると、制御チャネルおよびオプションで権限付きデータチャネルが接続されます。SVM が属するノードの FPolicy プロセスで、ファイルおよびフォルダに対するアクセスの監視が開始され、設定された条件に当てはまるイベントが見つかると、 FPolicy サーバ（ FPolicy サーバが設定されていない場合は標準のエンジン）に通知が送信されます。

ポリシーでネイティブファイルブロッキングを使用する場合は、外部エンジンは設定されず、関連付けられることもありません。

FPolicy 外部エンジンの設定を計画します

FPolicy 外部エンジンの設定を計画します

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を理解し、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（ 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
- ノードと FPolicy サーバ間の接続を認証する方法

  相互 SSL 認証を設定することを選択した場合は、 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。

。 `vserver fpolicy policy external-engine create` コマンドは、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、構成を計画するのに役立ちます。

情報のタイプ	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。これにより、外部エンジンがポリシーに関連付けられます。 この名前に指定できる文字数は最大 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の名前を設定する場合、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、ポリシーが有効にされ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、通知は各 FPolicy サーバにラウンドロビン方式で送信されます。 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での 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にも到達できない場合にのみ使用されます。ポリシーが有効になっている場合はセカンダリサーバへの接続が確立されますが、通知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セカンダリサーバに送信されます。複数のセカンダリ FPolicy サーバを設定した場合、通知は各 FPolicy サーバにラウンドロビン方式で送信されます。	`-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。 に設定すると `synchronous`ファイル要求処理ではFPolicyサーバに通知が送信されますが、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、 FPolicy サーバからの応答が要求されたアクションを許可するかどうかによって、要求フローが続行されるか処理が拒否されるかが決まります。 に設定すると `asynchronous`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`
_SSL オプションを使用して FPolicy サーバと通信します FPolicy サーバとの通信のための 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。 • に設定すると `no-auth`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。 • に設定すると `server-auth`SVMは、SSLサーバ認証を使用してFPolicyサーバを認証します。 • に設定すると `mutual-auth`では、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、も設定する必要があります `-certificate-common-name`、 `-certificate-serial`および `-certifcate-ca` パラメータ	`-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、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として指定できます。 を指定する場合 `mutual-auth` をクリックします `-ssl-option` パラメータを使用する場合は、に値を指定する必要があります `-certificate-common-name` パラメータ	`-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、認証に使用される証明書のシリアル番号を指定します。 を指定する場合 `mutual-auth` をクリックします `-ssl-option` パラメータを使用する場合は、に値を指定する必要があります `-certificate-serial` パラメータ	`-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、認証に使用される証明書の CA 名を指定します。 を指定する場合 `mutual-auth` をクリックします `-ssl-option` パラメータを使用する場合は、に値を指定する必要があります `-certificate-ca` パラメータ	`-certificate-ca text`

外部エンジンの詳細オプション

高度な FPolicy 設定パラメータの次の表は、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は、クラスタノードと FPolicy サーバ間の通信動作を変更するために使用します。

情報のタイプ	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 _ 時間間隔を時間単位で指定します (h）、分 (m）、または秒 (`s`ノードはFPolicyサーバからの応答を待機します。 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向上させることができます。また、通知要求がパフォーマンスの低い、またはダウンした FPolicy サーバから代替 FPolicy サーバへ移されているため、タイムアウトによってリクエストをキャンセルすることは、システムリソースを解放するのに役立ちます。 この値の範囲はです 0 から 100。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 _ タイムアウトを時間単位で指定します (h）、分 (m）、または秒 (s）をクリックして、要求を中止します。 この値の範囲はです 0 から 200。	-reqs-abort-timeout ` `integer[h
m	s]
ステータス要求の送信間隔 _ 間隔を時間単位で指定します (h）、分 (m）、または秒 (s）をクリックすると、FPolicyサーバにステータス要求が送信されます。 この値の範囲はです 0 から 50。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。 この値の範囲はです 1 から 10000。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 _ 時間間隔を時間単位で指定します (h）、分 (m）、または秒 (s）をクリックすると、FPolicyサーバへの接続が終了します。 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のみ、タイムアウト期間が経過したあとに接続を終了します。許可される要求の最大数はどちらかです 50 （デフォルト）またはで指定された番号 max-server-reqs- パラメータ この値の範囲はです 1 から 100。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 _ 時間間隔を時間単位で指定します (h）、分 (m）、または秒 (s）をクリックすると、FPolicyサーバにキープアライブメッセージが送信されます。 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。 この値の範囲はです 10 から 600。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できる最大回数を指定します。 この値の範囲はです 0 から 20。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ている値に設定されます。 たとえば、ソケットのデフォルト受信バッファサイズが 65 、 536 バイトの場合、この調整可能な値を 0 に設定すると、ソケットのバッファサイズは 65 、 536 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ている値に設定されます。 たとえば、ソケットのデフォルト送信バッファサイズが 65 、 536 バイトの場合、この調整可能な値を 0 に設定すると、ソケットのバッファサイズは 65 、 536 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 _ 間隔を時間単位で指定します (`h`）、分 (`m`）、または秒 (`s`）をクリックすると、再接続の試行時にFPolicyサーバに新しいセッションIDが送信されます。 ストレージコントローラとFPolicyサーバとの間の接続が終了して、で再接続が行われた場合 `-session-timeout` 間隔：古い通知に対する応答を送信できるように、古いセッション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` [`integer`H][`integer`M][`integer`S]

追加情報 **SSL** 認証接続を使用するための **FPolicy** 外部エンジンの設定について

SSL サーバへの接続時に追加情報を使用するように FPolicy 外部エンジンを設定する場合は、いくつかの FPolicy を把握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 サーバに接続する際に 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、次の手順を実行します。 FPolicy サーバ証明書に署名した 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。インストールした証明書を 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 が相互認証に使用している間に証明書を削除すると、その証明書を使用する、無効になった 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て、その新しい証明書を使用する FPolicy 外部エンジンを新規作成し、 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 の証明書をインストールします

FPolicyサーバ証明書への署名に使用したCAのパブリック証明書は、を使用してインストールします `security certificate install` コマンドにを指定します `-type` パラメータをに設定します `client-ca`。SVMの認証に必要な秘密鍵とパブリック証明書は、を使用してインストールします `security certificate install` コマンドにを指定します `-type` パラメータをに設定します `server`。

ID が保持されない設定の SVM ディザスタリカバリ関係では、証明書がレプリケートされません

FPolicy サーバへの接続確立時の 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複製されません。SVM 上の FPolicy 外部エンジンの設定は複製されますが、セキュリティ証明書は複製されません。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を設定するときにに選択した値 `-identity-preserve` のオプション `snapmirror create` コマンドは、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を決定します。

を設定した場合は `-identity-preserve` オプションをに設定します `true` （ID保持）。セキュリティ証明書の情報を含むFPolicy設定の詳細がすべて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、オプションをに設定した場合だけです `false` （非ID保持）。

MetroCluster および SVM ディザスタリカバリ設定を含むクラスタ対象 FPolicy 外部エンジンの制限事項

クラスタを対象とした FPolicy 外部エンジンは、クラスタ Storage Virtual Machine （ SVM ）をそのエンジンに割り当てることで作成できます。ただし、クラスタ対象の外部エンジンを MetroCluster または SVM ディザスタリカバリ設定で作成する場合は、 SVM が FPolicy サーバとの外部通信で使用する認証方式を選択する際にある種の制限が存在します。

外部 FPolicy サーバの作成時に選択できる認証オプションは、認証なし、 SSL サーバ認証、 SSL 相互認証の 3 つです。外部 FPolicy サーバがデータ SVM に割り当てられている場合は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。

設定	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）	はい。
MetroCluster または SVM ディザスタリカバリと、 SSL サーバ認証または SSL 相互認証を行うクラスタ対象 FPolicy 外部エンジン	いいえ

- SSL 認証を行うクラスタ対象 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、認証をまったく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は、 ONTAP により、 SSL 認証を行うクラスタ対象 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します

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的な設定に関する情報

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。

情報のタイプ	必須	含める	値を入力します
Storage Virtual Machine （ SVM ）名	はい。	はい。	
エンジン名	はい。	はい。	
プライマリ FPolicy サーバ	はい。	はい。	
ポート番号	はい。	はい。	
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	はい。	はい。	
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

外部エンジンを詳細パラメータで設定するには、 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。

情報のタイプ	必須	含める	値を入力します
要求をキャンセルするためのタイムアウト	いいえ		

要求を破棄するためにタイムアウトしました	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		
再接続時にセッション ID を破棄するためのタイムアウト	いいえ		

FPolicy イベントの設定を計画します

FPolicy イベントの設定の概要を計画します

FPolicy イベントを設定する前に、 FPolicy イベントを作成することの意味を理解する必要があります。イベントで監視するプロトコル、監視するイベント、使用するイベントフィルタを決定する必要があります。この情報は、設定する値を計画するのに役立ちます。

FPolicy イベントを作成することの意味

FPolicy イベントを作成することは、どのファイルアクセス操作を監視するか、またどの監視対象イベント通知を外部 FPolicy サーバに送信するかを決定するために、 FPolicy プロセスで必要となる情報を定義することを意味します。FPolicy イベントの設定では、次の設定情報を定義します。

- Storage Virtual Machine （ SVM ）名
- イベント名
- 監視するプロトコル

  FPolicy は、 SMB 、 NFSv3 、および NFSv4 のファイルアクセス処理を監視できます。

- 監視するファイル操作

すべてのファイル操作が各プロトコルに対して有効であるとは限りません。

- 構成するファイルフィルタ

  ファイル操作とフィルタの特定の組み合わせのみが有効です。各プロトコルには、サポートされる独自の組み合わせがあります。

- ボリュームのマウントおよびアンマウント操作を監視するかどうか

> 3つのパラメータには依存関係があります (`-protocol`、 `-file-operations`、 `-filters` ）。以下の組み合わせが 3 つのパラメータで有効です。
>
> - を指定できます `-protocol` および `-file-operations` パラメータ
> - 3 つのパラメータをすべて同時に指定することもできます。
> - いずれのパラメータも指定しないでください。

FPolicy イベント構成に含まれるもの

次に示す使用可能な FPolicy イベント設定パラメータの一覧は、構成を計画するのに役立ちます。

情報のタイプ	オプション
SVM この FPolicy イベントに関連付ける 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`
_ イベント名 _ FPolicy イベントに割り当てる名前を指定します。FPolicy ポリシーを作成する際には、イベント名を使用して FPolicy イベントをポリシーに関連付けます。 この名前に指定できる文字数は最大 256 文字です。 MetroCluster または SVM ディザスタリカバリ設定でイベントを設定する場合、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 “.”	`-event-name event_name`

プロトコル _ FPolicy イベント用に設定するプロトコルを指定します。のリスト `-protocol` 次のいずれかの値を指定できます。 • `cifs` • `nfsv3` • `nfsv4` を指定する場合 `-protocol`をクリックした場合は、で有効な値を指定する必要があります `-file-operations` パラメータプロトコルのバージョンによって、有効な値が変わる可能性があります。	`-protocol protocol`

_ ファイル操作 _ FPolicy イベントのファイル操作のリストを指定します。 イベントは、で指定されたプロトコルを使用して、すべてのクライアント要求からこのリストに指定された操作をチェックします `-protocol` パラメータ1 つ以上のファイル操作をカンマで区切って指定できます。のリスト `-file-operations` 次の値を1つ以上指定できます。 • `close` ファイルクローズ操作の場合 • `create` ファイル作成操作の場合 • `create-dir` ディレクトリ作成操作に使用します • `delete` ファイル削除操作に使用します • `delete_dir` ディレクトリ削除操作の場合 • `getattr` 属性取得操作の場合 • `link` リンク操作の場合 • `lookup` 検索操作に使用します • `open` ファイルオープン操作の場合 • `read` ファイル読み取り操作に使用します • `write` ファイル書き込み操作の場合 • `rename` ファイル名変更操作の場合 • `rename_dir` ディレクトリ名変更操作 • `setattr` 属性設定操作の場合 • `symlink` シンボリックリンク操作に使用します ⓘ を指定する場合 `-file-operations`をクリックした場合は、で有効なプロトコルを指定する必要があります `-protocol` パラメータ	`-file-operations` `file_operations`はい。

_ フィルタ _ 指定したプロトコルにおける所定のファイル操作に対するフィルタのリストを指定します。の値を指定します `-filters` パラメータは、クライアント要求をフィルタリングするために使用します。リストには次の値を 1 つ以上指定できます。 を指定する場合は `-filters` パラメータを指定すると、の有効な値も指定する必要があります `-file-operations` および `-protocol` パラメータ • `monitor-ads` 代替データストリームを要求するクライアント要求をフィルタリングするオプション。 • `close-with-modification` 変更してクローズ操作を要求するクライアント要求をフィルタリングするオプション。 • `close-without-modification` 変更せずにクローズ操作を要求するクライアント要求をフィルタリングするオプション。 • `first-read` 初回の読み取りを要求するクライアント要求をフィルタリングするオプション。 • `first-write` 初回の書き込みを要求するクライアント要求をフィルタリングするオプション。 • `offline-bit` オフラインビットの設定を要求するクライアント要求をフィルタリングするオプション。 このフィルタを設定すると、オフラインのファイルがアクセスされた場合のみ FPolicy サーバが通知を受信します。 • `open-with-delete-intent` 削除するためにファイルのオープンを要求するクライアント要求をフィルタリングするオプション。 このフィルタを設定すると、削除するためにファイルが開かれた場合のみ FPolicy サーバが通知を受信します。これは、ファイルシステムでが使用されるときに使用されます `FILE_DELETE_ON_CLOSE` フラグが指定されています。 • `open-with-write-intent` 書き込み目的でのオープン操作を要求するクライアント要求をフィルタリングするオプション。 このフィルタを設定すると、書き込むためにファイルを開いた場合のみ FPolicy サーバが通知を受信します。 • `write-with-size-change` 書き込みと同時にサイズの変更を要求するクライアント要求をフィルタリングするオプション。	`-filters` `filter`はい。

_ フィルタ _ 続き • `setattr-with-owner-change` ファイルまたはディレクトリの所有者を変更するクライアント属性設定要求をフィルタリングするオプション。 • `setattr-with-group-change` ファイルまたはディレクトリのグループを変更するクライアント属性設定要求をフィルタリングするオプション。 • `setattr-with-sacl-change` ファイルまたはディレクトリのSACLを変更するクライアント属性設定要求をフィルタリングします。 このフィルタは、SMBプロトコルとNFSv4プロトコルでのみ使用できます。 • `setattr-with-dacl-change` ファイルまたはディレクトリのDACLを変更するクライアント属性設定要求をフィルタリングします。 このフィルタは、SMBプロトコルとNFSv4プロトコルでのみ使用できます。 • `setattr-with-modify-time-change` ファイルまたはディレクトリの変更日時を変更するクライアント属性設定要求をフィルタリングするオプション。 • `setattr-with-access-time-change` ファイルまたはディレクトリのアクセス時間を変更するクライアント属性設定要求をフィルタリングするオプション。 • `setattr-with-creation-time-change` ファイルまたはディレクトリの作成日時を変更するクライアント属性設定要求をフィルタリングするオプション。 このオプションは、SMBプロトコルに対してのみ使用できます。 • `setattr-with-mode-change` オプション：ファイルまたはディレクトリのモードビットを変更するクライアント属性設定要求をフィルタリングします。 • `setattr-with-size-change` ファイルサイズを変更するクライアント属性設定要求をフィルタリングするオプション。 • `setattr-with-allocation-size-change` ファイルの割り当てサイズを変更するクライアント属性設定要求をフィルタリングするオプション。 このオプションは、SMBプロトコルに対してのみ使用できます。 • `exclude-directory` ディレクトリ操作を要求するクライアント要求をフィルタリングするオプション。 このフィルタを指定すると、ディレクトリ操作は監視されません。	`-filters` `filter`はい。

は、ボリューム処理が必要です _ ボリュームのマウントおよびアンマウント操作に対して監視が必要かどうかを指定します。デフォルトはです `false`。	`-volume-operation` {`true`
`false`} `-filters` `filter`はい。	*FPolicy*アクセスが通知を拒否しました ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。これらの通知は、セキュリティ、ランサムウェア対策、ガバナンスに役立ちます。権限がないためにファイル操作が失敗した場合は、次のような通知が生成されます。 • NTFS権限が原因でエラーが発生しました。 • UNIXモードビットによるエラー。 • NFSv4 ACLに起因するエラー。
`-monitor-fileop-failure` {`true`	`false`}

FPolicyで監視可能な、サポートされるファイル処理とフィルタの組み合わせ（**SMB**）

FPolicy イベントを設定する場合、 SMB のファイルアクセスの監視では、サポートされるファイル操作とフィルタの組み合わせに制限があることを考慮する必要があります。

以下の表に、 FPolicy による SMB ファイルアクセスイベントの監視でサポートされるファイル操作とフィルタの組み合わせを示します。

サポートされているファイル操作	サポートされているフィルタ
を閉じます	monitor-ads 、 offline-bit 、 close-with-modification 、 close-without-modification 、 close-with-read 、 exclude-directory
作成	monitor-ads 、 offline-bit
create_dir	現在、このファイル操作ではフィルタはサポートされていません。
削除	monitor-ads 、 offline-bit

delete_dir	現在、このファイル操作ではフィルタはサポートされていません。
属性の取得	offline-bit 、 exclud-dir のいずれかを指定します
を開きます	monitor-ads 、 offline-bit 、 open-with-delete-intent 、 open-with-write-intent 、 exclud-dir
読み取り	monitor-ads 、 offline-bit 、 first-read
書き込み	monitor-ads 、 offline-bit 、 first-write 、 write-with-size-change
名前を変更する	monitor-ads 、 offline-bit
rename_dir	現在、このファイル操作ではフィルタはサポートされていません。
属性の設定	monitor-ads 、 offline-bit 、 setattr_-with-owner_change 、 setattr_-with-group_change 、 setattr_-with-mode_change 、 setattr_-with_sacl_change 、 setattr_-with_dacl_change 、 setattr_-with-mody_time-change 、 setattr_-with-access-name_time-change 、 setattr_-with-creation_time-change 、 setattr-with_size_change 、 setattr_-with-allocation_size_change 、 exclude_directory

ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。次の表に、FPolicyによるSMBファイルアクセスイベントの監視でサポートされるアクセス拒否ファイル操作とフィルタの組み合わせを示します。

サポートされるアクセス拒否ファイル操作	サポートされているフィルタ
を開きます	NA

FPolicyで監視可能なサポートされるファイル処理とフィルタの組み合わせ（**NFSv3**）

FPolicyイベントを設定する場合、NFSv3のファイルアクセス操作の監視では、サポートされるファイル操作とフィルタの組み合わせに制限があることに注意する必要があります。

次の表に、FPolicyによるNFSv3ファイルアクセスイベントの監視でサポートされるファイル処理とフィルタの組み合わせを示します。

サポートされているファイル操作	サポートされているフィルタ
作成	オフラインビット
create_dir	現在、このファイル操作ではフィルタはサポートされていません。

削除	オフラインビット
delete_dir	現在、このファイル操作ではフィルタはサポートされていません。
リンク	オフラインビット
検索	offline-bit 、 exclud-dir のいずれかを指定します
読み取り	オフラインビット、初回読み取り
書き込み	オフラインビット、初回書き込み、 write-with-size-change
名前を変更する	オフラインビット
rename_dir	現在、このファイル操作ではフィルタはサポートされていません。
属性の設定	offline-bit 、 setattr_-with-owner_change 、 setattr_name_group-change 、 setattr_-with-mode_change 、 setattr_-with-mode_change 、 setattr_-with-mode_time-change 、 setattr_-with-access-time-change 、 setattr_-with-size_change 、 exclude_directory
シンボリックリンク	オフラインビット

ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。次の表に、FPolicyによるNFSv3ファイルアクセスイベントの監視でサポートされるアクセス拒否ファイル処理とフィルタの組み合わせを示します。

サポートされるアクセス拒否ファイル操作	サポートされているフィルタ
にアクセスします	NA
作成	NA
create_dir	NA
削除	NA
delete_dir	NA
リンク	NA
読み取り	NA

名前を変更する	NA
rename_dir	NA
属性の設定	NA
書き込み	NA

FPolicy で NFSv4 を監視するために、サポートされるファイル操作とフィルタの組み合わせ

FPolicy イベントを設定する場合、 NFSv4 のファイルアクセス操作の監視では、サポートされるファイル操作とフィルタの組み合わせに制限があることを考慮する必要があります。

以下の表に、 FPolicy による NFSv4 ファイルアクセスイベントの監視でサポートされるファイル操作とフィルタの組み合わせを示します。

サポートされているファイル操作	サポートされているフィルタ
を閉じます	offline-bit 、 exclude-directory
作成	オフラインビット
create_dir	現在、このファイル操作ではフィルタはサポートされていません。
削除	オフラインビット
delete_dir	現在、このファイル操作ではフィルタはサポートされていません。
属性の取得	offline-bit 、 exclude-directory
リンク	オフラインビット
検索	offline-bit 、 exclude-directory
を開きます	offline-bit 、 exclude-directory
読み取り	オフラインビット、初回読み取り
書き込み	オフラインビット、初回書き込み、 write-with-size-change

名前を変更する	オフラインビット
rename_dir	現在、このファイル操作ではフィルタはサポートされていません。
属性の設定	offline-bit 、 setattr_-with-owner_change 、 setattr_-with-group_change 、 setattr_-with-mode_change 、 setattr_-with-acl_change 、 setattr_-with_dacl_change 、 setattr_on_mode_time-change 、 setattr_-with-access-time-change 、 setattr_-with_size_change 、 exclude_directory
シンボリックリンク	オフラインビット

ONTAP 9.13.1以降では、権限がないためにファイル処理が失敗した場合に通知を受け取ることができます。次の表に、FPolicyによるNFSv4ファイルアクセスイベントの監視でサポートされるアクセス拒否ファイル操作とフィルタの組み合わせを示します。

サポートされるアクセス拒否ファイル操作	サポートされているフィルタ
にアクセスします	NA
作成	NA
create_dir	NA
削除	NA
delete_dir	NA
リンク	NA
を開きます	NA
読み取り	NA
名前を変更する	NA
rename_dir	NA
属性の設定	NA
書き込み	NA

FPolicy イベントの設定ワークシートに記入

このワークシートを使用して、 FPolicy イベント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、 FPolicy イベントを設定する前に、そのパラメータに使用する値を決定する必要があります。

FPolicy イベント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。

情報のタイプ	必須	含める	値を入力します
Storage Virtual Machine （ SVM ）名	はい。	はい。	
イベント名	はい。	はい。	
プロトコル	いいえ		
ファイル操作	いいえ		
フィルタ	いいえ		
ボリューム操作	いいえ		
アクセス拒否イベント+ （ONTAP 9.13以降でサポート）	いいえ		

FPolicy ポリシーの設定を計画します

FPolicy ポリシーの設定の概要を計画

FPolicy ポリシーを設定する前に、ポリシーの作成時に必要なパラメータや、特定のオプションパラメータを設定する理由について理解しておく必要があります。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 ポリシーを作成する際には、このポリシーと次のポリシーを関連付けます。

- Storage Virtual Machine （ SVM ）
- 1 つ以上の FPolicy イベント
- FPolicy 外部エンジン

いくつかのオプションポリシー設定を構成することもできます。

FPolicy ポリシーの設定項目

FPolicy ポリシーで使用できる必須パラメータとオプションパラメータを次に示します。これは設定について

計画するときに役立ちます。

情報のタイプ	オプション	必須	デフォルト
SVM 名 _ FPolicy ポリシーを作成する SVM の名前を指定します。	`-vserver vserver_name`	はい。	なし
_ ポリシー名 _ FPolicy ポリシーの名前を指定します。 この名前に指定できる文字数は最大 256 文字です。 MetroCluster または SVM ディザスタリカバリ設定でポリシーを設定する場合、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 “.”	`-policy-name policy_name`	はい。	なし
_ イベント名 _ FPolicy ポリシーに関連付けるイベントをカンマ区切りのリストで指定します。 • 1 つのポリシーに複数のイベントを関連付けることができます。 • イベントはプロトコルに固有です。 • 1 つのポリシーで複数のプロトコルのファイルアクセスイベントを監視するには、ポリシーで監視する各プロトコルのイベントを作成し、それらのイベントをポリシーに関連付けます。 • 既存のイベントを指定する必要があります。	`-events` `event_name`はい。	はい。	なし

_ 外部エンジン名 _ FPolicy ポリシーに関連付ける外部エンジンの名前を指定します。 • 外部エンジンには、ノードから FPolicy サーバに通知を送信するための必要な情報が格納されています。 • 単純なファイルブロッキングを行うために ONTAP の標準の外部エンジンを使用したり、より高度なファイルブロッキングとファイル管理を行うために外部 FPolicy サーバ（ FPolicy サーバ）を使用するように設定された外部エンジンを使用したりするように FPolicy を設定できます。 • 標準の外部エンジンを使用する場合は、このパラメータの値を指定しないか、を指定できます `native` を値として入力します。 • FPolicy サーバを使用する場合は、外部エンジンの設定がすでに存在している必要があります。	`-engine engine_name`	○（ポリシーで内部の ONTAP 標準エンジンを使用しない場合）	`native`
_ は必須のスクリーニングです _ 必須のファイルアクセススクリーニングを要求するかどうかを指定します。 • 必須のスクリーニング設定は、プライマリサーバとセカンダリサーバがすべて停止した場合や、指定した時間内に FPolicy サーバからの応答を得られない場合に、ファイルアクセスイベントをどのように処理するかを決定します。 • に設定すると `true`に設定すると、ファイルアクセスイベントが拒否されます。 • に設定すると `false`に設定すると、ファイルアクセスイベントが許可されます。	`-is-mandatory {true`	`false}`	いいえ

true	権限付きアクセスを許可する _ 権限付きデータ接続による監視対象のファイルやフォルダに対する権限付きアクセスを FPolicy サーバに許可するかどうかを指定します。 設定されている場合、 FPolicy サーバは権限付きデータ接続を使用して、監視対象データが格納されている SVM のルートにあるファイルにアクセスできます。 権限付きデータアクセスの場合は、クラスタでSMBのライセンスが有効になっていて、FPolicyサーバへの接続に使用されるすべてのデータLIFがに設定されている必要があります cifs 許可されているプロトコルの1つとして指定します。 ポリシーで権限付きアクセスを許可する場合は、 FPolicy サーバで権限付きアクセスに使用するアカウントのユーザ名も指定する必要があります。	-allow -privileged -access {yes	no}

No （パススルーリードが有効になっていない場合）	no	_ 特権ユーザ名 _ FPolicy サーバが権限付きデータアクセスで使用するアカウントのユーザ名を指定します。 • このパラメータの値は、「ドメイン \ ユーザ名」の形式にする必要があります。 • 状況 -allow -privileged -access がに設定されます `no` を指定すると、このパラメータに設定された値は無視されます。	-privileged -user-name user_name

No （権限付きアクセスが有効になっていない場合）	なし	_allow passthrough-read _ FPolicy サーバによってセカンダリストレージ（オフラインファイル）にアーカイブされているファイルを対象としたパススルーリードサービスを FPolicy サーバが提供できるかどうかを指定します。 • パススルーリードは、オフラインファイルのデータをプライマリストレージにリストアすることなく読み取るための手段です。 パススルーリードでは、読み取り要求に応答する前にファイルをプライマリストレージにリコールする必要がないため、応答遅延が短縮されます。また、パススルーリードでは、読み取り要求を満たすためだけにリコールされるファイルによってストレージ領域を浪費する必要がなくなるため、ストレージ効率が最適化されます。 • 有効になっている場合、FPolicy サーバはパススルーリード専用に開かれている別の権限付きデータチャネルを使用してファイルにデータを提供します。	`-is-passthrough-read-enabled` {`true`

FPolicy ポリシーで標準のエンジンを使用する場合の FPolicy スコープ設定の要件

標準のエンジンを使用するように FPolicy ポリシーを設定する場合には、ポリシーで設定される FPolicy スコープの定義方法に関して特定の要件があります。

FPolicy スコープは、 FPolicy 環境で指定されたボリュームや共有など、FPolicyポリシーが適用される範囲の境界を定義します。FPolicy ポリシーが適用されるスコープをさらに制限するためのパラメータが多数あります。次のいずれかのパラメータ `-is-file-extension-check-on-directories-enabled`では、ディレクトリのファイル拡張子をチェックするかどうかを指定します。デフォルト値はです `false`これは、ディレクトリ上のファイル拡張子はチェックされないことを意味します。

標準のエンジンを使用するFPolicyポリシーが共有またはボリュームおよびで有効になっている場合 `-is-file-extension-check-on-directories-enabled` パラメータはに設定されます `false` ポリシーのスコープでは、ディレクトリへのアクセスは拒否されます。この設定では、ディレクトリのファイル拡張子はチェックされないため、ポリシーのスコープ下にあるディレクトリ操作はすべて拒否されます。

標準のエンジンを使用している場合にディレクトリへのアクセスを成功させるには、を設定する必要があります `-is-file-extension-check-on-directories-enabled parameter` 終了： `true` 有効範囲の作成時。

（このパラメータはに設定されています） `true`では、ディレクトリ操作に対して拡張子のチェックが実行され、アクセスを許可するか拒否するかは、FPolicyスコープ設定に含まれている拡張子または除外されている拡張子に基づいて決定されます。

FPolicy ポリシーのワークシートに記入

このワークシートを使用して、 FPolicy ポリシー設定プロセス中に必要となる値を記録できます。FPolicy ポリシー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。

情報のタイプ	含める	値を入力します
Storage Virtual Machine （ SVM ）名	はい。	
ポリシー名	はい。	
イベント名	はい。	
外部エンジンの名前		
スクリーニングを必須にするかどうか		
権限付きアクセスを許可します		
権限を持つユーザの名前		
パススルーリードが有効かどうか		

FPolicy スコープの設定を計画します

FPolicy スコープの設定の概要を計画します

FPolicy スコープを設定する前に、スコープを作成することの意味を理解する必要があります。スコープの構成要素を理解する必要があります。また、スコープの優先規則についても理解する必要があります。この情報は、設定する値を計画するのに役立ちます。

FPolicy スコープを作成することの意味

FPolicy スコープを作成することは、 FPolicy ポリシーの適用範囲を定義することを意味します。Storage Virtual Machine （ SVM ）は基本の適用範囲です。FPolicy ポリシーのスコープを作成する場合、スコープが適用される FPolicy ポリシーを定義する必要があり、さらにスコープを適用する SVM を指定する必要があります。

指定した SVM 内にスコープをさらに制限するためのパラメータが数多くあります。スコープに含めるものを指定したり、スコープから除外するものを指定したりすることでスコープを制限することができます。有効なポリシーにスコープを適用すると、ポリシーイベントのチェックがこのコマンドで定義したスコープに適用されます。

「 include 」オプションで一致するファイルアクセスイベントが見つかった場合に、通知が生成されます。「 EXCLUDE 」オプションで一致するファイルアクセスイベントについては、通知は生成されません。

FPolicy スコープの構成では、次の設定情報を定義します。

- SVM 名
- ポリシー名
- 監視対象に含めるまたは監視対象から除外する共有
- 監視対象に含めるまたは監視対象から除外するエクスポートポリシー
- 監視対象に含めるまたは監視対象から除外するボリューム
- 監視対象に含めるまたは監視対象から除外するファイル拡張子
- ディレクトリオブジェクトに対してファイル拡張子を監視するかどうか

> クラスタの FPolicy ポリシーのスコープには、特に考慮すべき事項があります。クラスタの FPolicy ポリシーは、クラスタ管理者が管理 SVM 用に作成するポリシーです。クラスタ管理者がそのクラスタの FPolicy ポリシーのスコープも作成する場合、 SVM 管理者はそれと同じポリシーのスコープを作成することはできません。ただし、クラスタ管理者がクラスタの FPolicy ポリシーのスコープを作成しない場合は、すべての SVM 管理者がそのクラスタポリシーのスコープを作成することができます。SVM 管理者がそのクラスタの FPolicy ポリシーのスコープを作成した場合、クラスタ管理者はそれ以降、その同じクラスタポリシーのクラスタスコープを作成することはできません。これは、クラスタ管理者が同じクラスタポリシーのスコープを上書きできないためです。

スコープの優先規則

スコープの設定には、次の優先規則が適用されます。

- 共有がに含まれる場合 `-shares-to-include` 共有のパラメータと親ボリュームがに含まれます `-volumes-to-exclude` パラメータ `-volumes-to-exclude` が優先されます `-shares-to-include`。
- エクスポートポリシーがに含まれている場合 `-export-policies-to-include` エクスポートポリシーのパラメータと親ボリュームがに含まれます `-volumes-to-exclude` パラメータ `-volumes-to-exclude` が優先されます `-export-policies-to-include`。
- 管理者は両方を指定できます `-file-extensions-to-include` および `-file-extensions-to-exclude` リスト。

  。 `-file-extensions-to-exclude` パラメータは、の前にチェックされます `-file-extensions-to-include` パラメータがチェックされています。

FPolicy スコープの構成要素を次に示します

次に示す使用可能な FPolicy スコープの設定パラメータの一覧は、構成を計画するのに役立ちます。

> スコープに含めるか除外する共有、エクスポートポリシー、ボリューム、およびファイル拡張子を設定する際に、includeパラメータとexcludeパラメータにメタ文字（「'」など）を含めることができます?`" and “*”。 正規表現の使用はサポートされていません。

情報のタイプ	オプション
SVM FPolicy スコープを作成する 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`
_ ポリシー名 _ スコープをアタッチする FPolicy ポリシーの名前を指定します。FPolicy ポリシーがすでに存在している必要があります。	`-policy-name policy_name`
含める共有 _ カンマで区切って複数の共有を指定し、 FPolicy ポリシーの監視対象となるスコープに含めます。	`-shares-to-include` `share_name`はい。
_ 除外する共有 _ カンマで区切って複数の共有を指定し、 FPolicy ポリシーの監視対象となるスコープから除外します。	`-shares-to-exclude` `share_name`はい。
対象に含めるボリューム： FPolicy ポリシーの監視対象となるボリュームをカンマで区切って指定します。	`-volumes-to-include` `volume_name`はい。

除外するボリューム _ カンマで区切って複数のボリュームを指定し、 FPolicy ポリシーの監視対象となるスコープから除外します。	`-volumes-to-exclude` `volume_name`はい。
ポリシーを含めるには _ をエクスポートします カンマで区切って複数のエクスポートポリシーを指定し、 FPolicy ポリシーの監視対象となるスコープに含めます。	`-export-policies-to-include` `export_policy_name`はい。
ポリシーを exclude_ にエクスポートします カンマで区切って複数のエクスポートポリシーを指定し、 FPolicy ポリシーの監視対象となるスコープから除外します。	`-export-policies-to-exclude` `export_policy_name`はい。
_include するファイル拡張子 _ カンマで区切って複数のファイル拡張子を指定し、 FPolicy ポリシーの監視対象となるスコープに含めます。	`-file-extensions-to-include` `file_extensions`はい。
_ ファイル拡張子を exclude_ に設定します カンマで区切って複数のファイル拡張子を指定し、 FPolicy ポリシーの監視対象となるスコープから除外します。	`-file-extensions-to-exclude` `file_extensions`はい。
_ ディレクトリのファイル拡張子チェックは有効になっていますか？ _ ファイル名の拡張子の監視をディレクトリオブジェクトに適用するかどうかを指定します。このパラメータがに設定されている場合 `true`の場合、ディレクトリオブジェクトには、通常のファイルと同じ拡張子チェックが適用されます。このパラメータがに設定されている場合 `false`では、ディレクトリ名の拡張子は照合されず、名前の拡張子が一致しない場合でも、ディレクトリに関する通知が送信されます。 スコープの割り当て先のFPolicyポリシーが標準のエンジンを使用するように設定されている場合は、このパラメータをに設定する必要があります `true`。	`-is-file-extension-check-on-directories-enabled` {`true`
`false`	}

FPolicy スコープのワークシートに情報を記入します

このワークシートを使用して、 FPolicy スコープ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、 FPolicy スコープを設定する前に、そのパラメータに使用する値を決定する必要があります。

FPolicy スコープ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。

情報のタイプ	必須	含める	値を入力します
Storage Virtual Machine （ SVM ）名	はい。	はい。	
ポリシー名	はい。	はい。	
対象に含める共有	いいえ		
対象から除外する共有	いいえ		
対象に含めるボリューム	いいえ		
ボリュームを除外する	いいえ		
エクスポートポリシーを含める	いいえ		
エクスポートポリシーを除外する	いいえ		
対象に含めるファイル拡張子	いいえ		
対象から除外するファイル拡張子	いいえ		
ディレクトリのファイル拡張子の監視が有効かどうか	いいえ		