



FPolicy設定を計画する ONTAP 9

NetApp
December 20, 2024

目次

FPolicy設定を計画する	1
FPolicyの設定に関する要件、考慮事項、およびベストプラクティス	1
FPolicy設定手順とは	7
FPolicy外部エンジンの設定を計画する	8
FPolicyイベントの設定を計画する	18
FPolicyポリシーの設定を計画する	28
FPolicyスコープの設定を計画する	35

FPolicy設定を計画する

FPolicyの設定に関する要件、考慮事項、およびベストプラクティス

Storage Virtual Machine (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は`data-fpolicy-client`サービスを追加することでアウトバウンドFPolicy接続用のクライアントLIFサービスを提供しています。["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"](#)です。

- 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サーバが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経由で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サーバは、FPolicyの設定で設定されたクレデンシャルで実行されている必要があります。
 - FPolicyサーバとの通信に使用されるすべてのデータLIFが、許可されているプロトコルの1つとして設定されている必要があります `cifs`。

これには、パススルーリード接続に使用されるLIFも含まれます。

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。

永続的ストア

ONTAP 9.14.1以降では、FPolicyを使用して永続的ストアを作成し、SVM内の非同期で必須で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できます。永続的ストアは、クライアントI/O処理をFPolicy通知処理から分離して、クライアントのレイテンシを低減するのに役立ちます。同期（必須かどうかは問わない）および非同期で必須の設定はサポートされていません。

- 永続的ストア機能を使用する前に、この設定がパートナー アプリケーションでサポートされていることを確認してください。
- FPolicyが有効になっているSVMごとに永続的ストアが1つ必要です。
 - 各SVMに設定できる永続的ストアは1つだけです。ポリシーが別々のパートナーのものであっても、この単一の永続的ストアをそのSVM上のすべてのFPolicy設定に使用する必要があります。
- ONTAP 9.15.1以降：
 - 永続的ストア、そのボリューム、およびボリューム設定は、永続的ストアの作成時に自動的に処理されます。
- ONTAP 9.14.1：
 - 永続的ストア、そのボリューム、およびボリューム設定は手動で処理します。
- 永続的ストアのボリュームは、FPolicyによって監視されるトラフィック量が最大になると想定されるLIFがあるノードに作成します。
 - ONTAP 9.15.1以降：永続的ストアの作成時にボリュームが自動的に作成および設定されます。
 - ONTAP 9.14.1：クラスタ管理者は、FPolicyが有効になっている各SVMで永続的ストア用のボリュームを作成し、設定する必要があります。
- 永続的ストアに蓄積された通知がプロビジョニングされたボリュームのサイズを超えると、FPolicyは適切なEMSメッセージを含む受信通知を破棄し始めます。
 - ONTAP 9.15.1以降：パラメータに加えて `size`、`'autosize-mode'` パラメータを使用すると、使用済みスペースの量に応じてボリュームを拡張または縮小できます。
 - ONTAP 9.14.1：この `'size'` パラメータは、ボリュームの作成時に最大数を指定するように設定されます。
- 永続的ストアボリュームのSnapshotポリシーをではなくに `default` 設定します `'none'`。これは、Snapshotが誤ってリストアされて現在のイベントが失われることがないようにし、イベント処理が重複しないようにするためです。
 - ONTAP 9.15.1以降：`'snapshot-policy'` 永続ストアの作成時に、パラメータは自動的に `none` に設定されます。
 - ONTAP 9.14.1：`snapshot-policy` ボリュームの作成時にパラメータがに設定されます `'none'`。
- 永続的なイベントレコードが誤って破損したり削除されたりしないように、外部ユーザプロトコルアクセ

ス (CIFS / NFS) で永続的ストアボリュームにアクセスできないようにします。

- ONTAP 9.15.1以降：ONTAPは、永続的ストアの作成時に外部ユーザプロトコルアクセス (CIFS / NFS) からボリュームを自動的にブロックします。
- ONTAP 9.14.1：FPolicyを有効にしたら、ONTAPでボリュームをアンマウントしてジャンクションパスを削除します。これにより、外部ユーザプロトコルによるアクセス (CIFS / NFS) ができなくなります。

詳細については、およびを参照して "[FPolicyの永続的ストア](#)" "[永続ストアの作成](#)" ください。

永続的ストアのフェイルオーバーとギブバック

永続ストアは、最後のイベントを受信したとき、予期しないリブートが発生したとき、またはFPolicyを無効にして再度有効にしたときのみです。テイクオーバー処理が完了すると、新しいイベントがパートナーノードに格納されて処理されます。ギブバック処理のあと、ノードのテイクオーバーの発生時に残っている可能性がある未処理のイベントの処理が永続的ストアで再開されます。ライブイベントは、未処理のイベントよりも優先されます。

永続的ストアボリュームが同じSVM内のノード間で移動した場合、まだ処理されていない通知も新しいノードに移動します。保留中の通知が外部サーバに配信されるようにするには、ボリュームの移動後にどちらかのノードでコマンドを再実行する必要がありますが `fpolicy persistent-store create` あります。

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パラメータがに設定されて true` いる場合 `is-file-extension-check-on-directories-enabled`、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実行されます。

ネットワーク設定

FPolicyサーバとコントローラ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、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回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は、適切な値を見極めるためにパートナーと協力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優先され、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、適切な優先度を見極めるためにパートナーと協力することを推奨しています。

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）に基づいて応答を待ちます。このプロセスは、SMBとNFSのアクセスとCPUリソースのパフォーマンスに影響します。

何らかの問題につながる可能性を抑えるため、NetAppは、FPolicyを有効にする前にパートナーと協力して環境の評価とサイジングを行う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、複数の要因から影響を受けます。

パフォーマンスの監視

FPolicyは、通知ベースのシステムです。通知は外部サーバに送信され、そこで処理され、生成された応答がONTAPに返されます。この往復プロセスにより、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ことで、ソリューション内のボトルネックを特定し、必要に応じてパラメータを調整してソリューションを最適化できます。たとえば、FPolicyのレイテンシの増加は、連鎖的にSMBとNFSのアクセス レイテンシに影響を及ぼします。そのため、ワークロード（SMBとNFS）とFPolicyのレイテンシのどちらも監視する必要があります。加えて、ONTAPのサービス品質（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やSVMごとにワークロードの設定を行います。

NetAppでは、コマンドを実行してワークロードの統計情報を表示することを推奨 `statistics show -object workload` 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 / 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ために、次のFPolicyカウンタを使用できます。



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。

- `statistics start -object fpolicy -instance instance_name -sample-id ID`
- `statistics start -object fpolicy_policy -instance instance_name -sample-id ID`

2. FPolicyカウンタを表示します。

- `statistics show -object fpolicy -instance instance_name -sample-id ID`
- `statistics show -object fpolicy_server -instance instance_name -sample-id ID`

`fpolicy`カウンタと
`fpolicy_server`カウンタには、次の表に示す複数のパフォーマンスパラメータに関する情報が表示されます。

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
通知の原因になったイベントのリスト	max_request_latency
スクリーニング要求の最大レイテンシ	outstanding_requests
処理中のスクリーン要求の総数	processed_requests
SVMでFPolicyの処理が完了したスクリーニング要求の総数	request_latency_hist
スクリーニング要求のレイテンシのヒストグラム	requests_dispatched_rate
送信されたスクリーニング要求の1秒あたりの数	requests_received_rate

カウンタ	説明
受信したスクリーニング要求の1秒あたりの数	「 fpolicy_server 」カウンタ
max_request_latency	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	スクリーニング要求の平均レイテンシ
request_latency_hist	スクリーニング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スクリーニング要求の1秒あたりの数
response_received_rate	FPolicyサーバから受信したスクリーニング応答の1秒あたりの数

FPolicyのワークフローと他のテクノロジーへの依存の管理

NetApp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、有効になっているポリシーに設定された外部エンジンのIPアドレスを追加または変更する場合は、まず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、NetAppは、読み取りと属性取得のファイル処理を監視するようにFPolicyを設定しないことを推奨しています。これらの処理をONTAPで監視するには、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ボリュームからは取得できないため、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で得られるパフォーマンス上のメリットが帳消しになってしまいます。

FPolicyと外部のウイルス対策ソリューションを両方とも導入している場合、最初にウイルス対策ソリューションが通知を受信します。FPolicyの処理は、ウイルス対策スキャンの完了後に開始されます。ウイルス対策スキャナが低速だと全体的なパフォーマンスに影響する可能性があるため、ウイルス対策ソリューションの適切なサイジングが重要になります。

パススルー リードのアップグレードと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。

アップグレード

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たうえで、設定を再び有効にする必要があります。

リバート

FPolicyをサポートしていないONTAPのバージョンにリバートする前に、以下の条件を満たす必要があります。

- パススルー リードを使用しているすべてのポリシーを無効にしたうえで、影響を受ける設定を変更してパススルー リードを使用しないようにする必要があります。

- クラスタ上のすべての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にリポートする前に、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、リポートは失敗します。

FPolicy設定手順とは

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。

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。詳細については、を参照してください。 "[FPolicy外部エンジンの設定を計画する](#)"

2. FPolicyイベントを作成します。

FPolicyイベントは、FPolicyポリシーで監視する対象を定義します。イベントは監視対象のプロトコルとファイル操作で構成され、一連のフィルタを含めることができます。イベントでは、フィルタを使用して、FPolicy外部エンジンから通知を送信する必要がある監視対象イベントのリストを絞り込みます。イベントは、ポリシーがボリューム操作を監視するかどうかも指定します。

3. FPolicy永続ストアを作成します（オプション）。

14.1以降では、ONTAP 9の必須ではない非同期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ようにを設定でき"[永続的ストア](#)"ます。同期（必須または非必須）および非同期の必須構成はサポートされていません。

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。

ONTAP 9 .15.1以降では、FPolicyの永続的ストアの設定が簡素化されています。 ``persistent-store-create`` コマンドは、SVM用のボリュームの作成を自動化し、永続的ストア用のボリュームを設定します。

4. 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な一般的なユースケースには、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、ある特定のSVMに複数のFPolicyポリシーを含めることは可能で、範囲、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。

5. ポリシーの範囲を設定します。

FPolicyスコープでは、ボリューム、共有、またはエクスポート ポリシーについて、ポリシーで監視するものと除外するものを指定します。また、ファイル拡張子についても、FPolicyの監視対象に含めるものと除外するものを指定します。



除外リストの方が対象リストよりも優先されます。

6. 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特権データ チャネル（オプション）の接続が確立されます。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ったら、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
<p>SVM</p> <p>この外部エンジンに関連付けるSVMの名前を指定します。</p> <p>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。</p>	<p><code>-vserver vserver_name</code></p>

<p>_ エンジン名 _</p> <p>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。</p> <p>名前の最大文字数は256文字です。</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>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。</p> </div> <p>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。</p> <ul style="list-style-type: none"> • a`から `z • A`から `Z • 0`から `9 • “_”、“-”、”、 and ” 	<p>-engine-name engine_name</p>
<p>プライマリ FPolicy サーバ _</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>-primary-servers `IP_address`はい。</p>
<p>ポート番号 _</p> <p>FPolicyサービスのポート番号を指定します。</p>	<p>-port integer</p>

<p><u>_ セカンダリ FPolicy サーバ _</u></p> <p>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。</p> <p>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。</p>	<pre>-secondary-servers `IP_address`はい。</pre>
<p><u>_ 外部エンジンタイプ _</u></p> <p>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。</p> <p>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。</p> <p>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。</p>	<pre>-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。</pre> <ul style="list-style-type: none"> • synchronous • asynchronous
<p>外部エンジンフォーマット</p> <p>外部エンジン形式がXMLかprotobufかを指定します。</p> <p>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。</p>	<pre>- extern-engine-format {protobuf または xml}</pre>

<p><u>_ SSL オプションを使用して FPolicy サーバと通信します</u></p> <p>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。</p> <ul style="list-style-type: none"> • に設定する `no-auth` と、認証は行われません。 <p>通信リンクはTCPを介して確立されます。</p> <ul style="list-style-type: none"> • 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。 <p>相互SSL認証を設定する場合は、`-certificate-serial`、の`-certificate-ca`各パラメータも設定する必要があります ` -certificate-common-name`。</p>	<pre>-ssl-option{no-auth</pre>
<pre>server-auth</pre>	<pre>mutual-auth}</pre>
<p><u>_ 証明書 FQDN またはカスタム共通名 _</u></p> <p>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。</p> <p>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`。</p>	<pre>-certificate-common-name text</pre>
<p><u>証明書シリアル番号 _</u></p> <p>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。</p> <p>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`。</p>	<pre>-certificate-serial text</pre>
<p><u>_ 認証局 _</u></p> <p>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。</p> <p>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`。</p>	<pre>-certificate-ca text</pre>

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
<p><u>リクエストをキャンセルするためのタイムアウト</u></p> <p>(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。</p> <p>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せん。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。</p> <p>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。</p>	<p>-reqs-cancel-timeout integer[h]</p>
<p>m</p>	<p>s]</p>
<p><u>要求を破棄するためのタイムアウト</u></p> <p>(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。</p> <p>この値の範囲は~ 200`です `0。</p>	<p>-reqs-abort-timeout ` integer[h]</p>
<p>m</p>	<p>s]</p>
<p><u>ステータス要求の送信間隔</u></p> <p>(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。</p> <p>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。</p>	<p>-status-req-interval integer[h]</p>
<p>m</p>	<p>s]</p>
<p><u>FPolicyサーバの未処理要求の最大数</u></p> <p>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。</p> <p>この値の範囲は~ 10000`です `1。デフォルトはです 500。</p>	<p>-max-server-reqs integer</p>

<p><u> 応答しない FPolicy サーバを切断するタイムアウト </u></p> <p>(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。</p> <p>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 <code>max-server-reqs-</code> です `50。</p> <p>この値の範囲は~ 100` です `1。デフォルトはです 60s。</p>	<pre>-server-progress -timeout integer[h</pre>
<p>m</p>	<p>s]</p>
<p><u> FPolicy サーバにキープアライブメッセージを送信する間隔 </u></p> <p>(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。</p> <p>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。</p> <p>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。</p>	<pre>-keep-alive-interval-integer[h</pre>
<p>m</p>	<p>s]</p>
<p><u> 最大再接続試行回数 </u></p> <p>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。</p> <p>この値の範囲は~ 20` です `0。デフォルトはです 5。</p>	<pre>-max-connection-retries integer</pre>
<p><u> 受信バッファサイズ </u></p> <p>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。</p> <p>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。</p> <p>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。</p>	<pre>-recv-buffer-size integer</pre>

<p>送信バッファサイズ <code>_</code></p> <p>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。</p> <p>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。</p> <p>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。</p>	<pre>-send-buffer-size integer</pre>
<p><code>_</code> 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 <code>_</code></p> <p>(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。</p> <p>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。</p> <p>デフォルト値は10秒に設定されています。</p>	<pre>-session-timeout [h][m]integerintegerinteg er</pre>

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	○	○	
プライマリ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		

FPolicyイベントの設定を計画する

FPolicyイベントの設定の概要を計画する

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、および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、NFSv4のファイルアクセス処理を監視できます。ONTAP 9.15.1以降では、NFSv4.1のファイルアクセス処理も監視できます。

- 監視するファイル処理

すべてのファイル処理が、各プロトコルに対して有効とは限りません。

- 構成するファイル フィルタ

ファイル処理とフィルタの特定の組み合わせだけが有効です。プロトコルごとに、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(-protocol、-file-operations、-filters) との依存関係があります。3つのパラメータの有効な組み合わせは次のとおりです。



- パラメータと -file-operations`パラメータを指定できます ` -protocol。
- 3つのパラメータをすべて指定できます。
- パラメータはどれも指定できません。

FPolicyイベントの設定内容

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、設定を計画するのに役立ちます。

情報の種類	オプション
<p>SVM</p> <p>このFPolicyイベントに関連付けるSVMの名前を指定します。</p> <p>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。</p>	<p>-vserver vserver_name</p>
<p>_ イベント名 _</p> <p>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ときは、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。</p> <p>名前の最大文字数は256文字です。</p> <p> 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。</p> <p>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。</p> <ul style="list-style-type: none"> • a`から `z • A`から `Z • 0`から `9 • _`、"、"、"、"-`、 and " 	<p>-event-name event_name</p>

プロトコル _

-protocol protocol

FPolicyイベントに設定するプロトコルを指定します。のリスト`-protocol`には、次のいずれかの値を指定できます。

- cifs
- nfsv3
- nfsv4



を指定する場合は `-protocol`、パラメータに有効な値を指定する必要があります `-file-operations`。プロトコルのバージョンが変わると、有効な値が変わることがあります。



NFSv4.15.1以降でONTAP 9は、NFSv4でNFSv4.0およびNFSv4.1のイベントをキャプチャできます。

_ 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。

このイベントは、パラメータで指定し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`。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` には、次の値を1つ以上指定できます。

- ``close`` ファイルクローズソウサ
- ``create`` ファイルサクセイソウサ
- ``create-dir`` ディレクトリサクセイソウサ
- ``delete`` ファイルサクジョソウサ
- ``delete_dir`` ディレクトリサクジョソウサ
- ``getattr`` 属性取得操作
- ``link`` リンクソウサ
- ``lookup`` ケンサクソウサ
- ``open`` ファイルオープンソウサ
- ``read`` ファイルヨミトリソウサ
- ``write`` ファイルカキコミソウサ
- ``rename`` ファイルメイヘンコウソウサ
- ``rename_dir`` ディレクトリメイヘンコウソウサ
- ``setattr`` 属性設定操作用
- ``symlink`` シンホリツクリンクソウサ



を指定する場合は `-file-operations`、パラメータに有効なプロトコルを指定する必要があります `-protocol`。

`-file-operations`
``file_operations`` はい。

_ フィルタ _

-filters `filter`はい。

指定したプロトコルの指定したファイル操作に対するフィルタのリストを指定します。パラメータの値`-filters`は、クライアント要求をフィルタリングするために使用されます。このリストには、次の1つ以上を指定できます。



パラメータを指定する場合`-filters`は、パラメータと`-protocol`パラメータに有効な値も指定する必要があります`-file-operations`。

- `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ときにのみ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を開こうとした場合にのみFPolicyサーバが通知を受信します。これは、フラグが指定されたときにファイルシステムによって使用されます

FILE_DELETE_ON_CLOSE。

- `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こうとした場合にのみ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。
- `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。

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 false。	-volume-operation{true
false} -filters `filter`はい。	<i>FPolicy</i> 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。権限不足でファイル処理が失敗した場合、次のメッセージを含む通知が生成されます。 <ul style="list-style-type: none"> • Failures due to NTFS permissions. • Failures due to Unix mode bits. • Failures due to NFSv4 ACLs.
-monitor-fileop-failure{true	false}

FPolicy `exclude-directory` オプションは、ディレクトリ操作を要求するファイルアクセスを拒否するフィルタリングのオプションです。

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。*FPolicy* イベントを設定する場合、SMB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
閉じる	monitor-ads、offline-bit、close-with-modification、close-with-modification、close-with-read、exclude-directory
作成	モニター広告、オフラインビット
create_dir	現在、このファイル処理でサポートされるフィルタはありません。

delete	モニター広告、オフラインビット
delete_dir	現在、このファイル処理でサポートされるフィルタはありません。
属性の取得	オフラインビット、exclude-dir
オープン	monitor-ads、offline-bit、open-with-delete-intent、open-with-write-intent、exclude-dir
読み取り	モニター広告、オフラインビット、初回読み取り
書き込み	monitor-ads、offline-bit、first-write、write-with-size-change
rename	モニター広告、オフラインビット
rename_dir	現在、このファイル処理でサポートされるフィルタはありません。
属性の設定	monitor-ads、offline-bit、setattr_with_owner_change、setattr_with_group_change、setattr_with_sacl_change、setattr_with_modify_time_change、setattr_with_access_time_change、setattr_with_creation_time_change、setattr_with_exclude、

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。以下の表に、FPolicyによるSMBファイル アクセス イベントの監視でアクセス拒否時に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
オープン	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、このファイル処理でサポートされるフィルタはありません。
delete	オフラインビット
delete_dir	現在、このファイル処理でサポートされるフィルタはありません。
リンク	オフラインビット
検索	オフラインビット、exclude-dir
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、first-write、write-with-size-change
rename	オフラインビット
rename_dir	現在、このファイル処理でサポートされるフィルタはありません。
属性の設定	オフラインビット、setattr_with_owner_change、setattr_with_group_change、setattr_with_mode_change、setattr_with_modify_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
アクセス	NA
作成	NA
create_dir	NA
delete	NA
delete_dir	NA
リンク	NA

読み取り	NA
rename	NA
rename_dir	NA
属性の設定	NA
書き込み	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 (NFSv4)

FPolicyイベントを設定する際には、NFSv4のファイルアクセス処理の監視では特定のファイル処理とフィルタの組み合わせだけがサポートされることを考慮する必要があります。

ONTAP 9 .15.1以降では、FPolicyはNFSv4.1プロトコルをサポートしています。

次の表に、FPolicyによるNFSv4またはNFSv4.1の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
閉じる	オフラインビット、exclude-directory
作成	オフラインビット
create_dir	現在、このファイル処理でサポートされるフィルタはありません。
delete	オフラインビット
delete_dir	現在、このファイル処理でサポートされるフィルタはありません。
属性の取得	オフラインビット、exclude-directory
リンク	オフラインビット
検索	オフラインビット、exclude-directory
オープン	オフラインビット、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、first-write、write-with-size-change
rename	オフラインビット
rename_dir	現在、このファイル処理でサポートされるフィルタはありません。
属性の設定	オフラインビット、setattr_with_owner_change、setattr_with_group_change、setattr_with_mode_change、setattr_with_sacl_change、setattr_with_modify_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。以下の表に、FPolicyによるNFSv4またはNFSv4.1ファイル アクセス イベントの監視でアクセス拒否時に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
アクセス	NA
作成	NA
create_dir	NA
delete	NA
delete_dir	NA
リンク	NA
オープン	NA
読み取り	NA
rename	NA
rename_dir	NA
属性の設定	NA
書き込み	NA

FPolicyイベント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。

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。

情報の種類	必須	含める	自分の価値観
Storage Virtual Machine (SVM) 名	○	○	
イベント名	○	○	
プロトコル	いいえ		
ファイルソウサ	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以降のサポート)	いいえ		

FPolicyポリシーの設定を計画する

FPolicyポリシーの設定の概要を計画する

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と、特定のオプションパラメータを設定する理由を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ときは、このポリシーを次のように関連付けます。

- 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のポリシー設定を構成することもできます。

FPolicyポリシーの設定内容

FPolicyポリシーの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、設定を計画するのに役

立ちます。

情報の種類	オプション	必須	デフォルト
<p>SVM 名 _</p> <p>FPolicyポリシーを作成するSVMの名前を指定します。</p>	<p>-vserver vserver_name</p>	○	なし
<p>_ ポリシー名 _</p> <p>FPolicyポリシーの名前を指定します。</p> <p>名前の最大文字数は256文字です。</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">  <p>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。</p> </div> <p>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。</p> <ul style="list-style-type: none"> • a`から `z • A`から `Z • 0`から `9 • “_”、“.”、“-”, and “ ” 	<p>-policy-name policy_name</p>	○	なし
<p>_ イベント名 _</p> <p>FPolicyポリシーに関連付けるイベントをカンマで区切って指定します。</p> <ul style="list-style-type: none"> • 1つのポリシーに複数のイベントに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。 	<p>-events `event_name`はい。</p>	○	なし

<p>永続ストア</p> <p>ONTAP 9.14.1以降では、このパラメータは、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永続ストアを指定します。</p>	<p>-persistent -store persistent_store_name</p>	<p>いいえ</p>	<p>なし</p>
<p>_ 外部エンジン名 _</p> <p>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。</p> <ul style="list-style-type: none"> 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に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、値としてを指定できます native。 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。 	<p>-engine engine_name</p>	<p>○（ポリシーで内部のONTAP標準エンジンを使用しない場合）</p>	<p>native</p>
<p>_ は必須のスクリーニングです _</p> <p>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。</p> <ul style="list-style-type: none"> この必須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 `true` 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 `false` と、ファイルアクセスイベントが許可されます。 	<p>-is-mandatory {true</p>	<p>false}</p>	<p>いいえ</p>

<p>true</p>	<p>権限付きアクセスを許可する _</p> <p>権限付きデータ接続を使用した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。</p> <p>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。</p> <p>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る必要があります。FPolicyサーバへの接続に使用されるすべてのデータLIFが、許可されているプロトコルの1つとして設定されている必要があります。`cifs` ます。</p> <p>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。</p>	<p>-allow -privileged -access{yes</p>	<p>no}</p>
-------------	---	---	------------

<p>× (パススルーリードが有効になっていない場合)</p>	<p>no</p>	<p><u>特権ユーザ名</u></p> <p>FPolicyサーバが権限付きデータアクセスに使用するアカウントのユーザ名を指定します。</p> <ul style="list-style-type: none"> 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。 がに設定されてno`いる場合`-allow-privileged-access、このパラメータに設定されている値は無視されます。 	<p>-privileged -user-name user_name</p>
---------------------------------	-----------	---	---

<p>× (権限付きアクセスが有効になっていない場合)</p>	<p>なし</p>	<p><code>_allow passthrough-read _</code></p> <p>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) にアーカイブされたファイルに対して、FPolicyサーバがパススルーリードサービスを提供できるかどうかを指定します。</p> <ul style="list-style-type: none"> 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方法です。 <p>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、応答レイテンシが短縮されます。さらに、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プライマリストレージスペースを消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。</p> <ul style="list-style-type: none"> 有効にすると、FPolicyサーバはパススルーリード専用に開かれた別の権限付きデータチャネルを介してファイルのデータを提供します。 	<pre>-is-passthrough -read-enabled {true</pre>
---------------------------------	-----------	--	--

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

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。これらのパラメータの1つで、`-is-file-extension-check-on-directories-enabled` 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 `false`、ディレクトリ上のファイル拡張子はチェックされません。

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で有効になっている場合、`-is-file-extension-check-on-directories-enabled` ポリシーのスコープでパラメータが設定されている `false` と、ディレクトリへのアクセスが拒否されます。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に該当す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、スコープの作成時に `true` に設定する必要があります。 `-is-file-extension-check-on-directories-enabled parameter` ます。

このパラメータを設定する `true` と、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ポリシーの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。

情報の種類	含める	自分の価値観
Storage Virtual Machine (SVM) 名	<input type="radio"/>	
ポリシー名	<input type="radio"/>	
イベント名	<input type="radio"/>	
永続的ストア		
外部エンジン名		
スクリーニングを必須にするかどうか		
特権アクセスを許可するかどうか		
特権ユーザの名前		

FPolicyスコープの設定を計画する

FPolicyスコープ設定の概要を計画する

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しておく必要があります。スコープ構成に含まれる内容を理解しておく必要があります。また、スコープの優先規則についても理解しておく必要があります。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ポリシーが適用される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ときは、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多数あります。スコープに含めるものを指定するか、スコープから除外するものを指定することで、スコープを制限できます。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スコープの設定では、次の設定情報を定義します。

- SVM名
- ポリシー名
- 監視対象に含める共有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するファイル拡張子のチェックを実行するかどうか



クラスタのFPolicyポリシーのスコープには、特別な考慮事項があります。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管理者はその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とは

スコープ設定には、次の優先規則が適用されます。

- 共有をパラメータに指定し、共有の親ボリュームをパラメータに `-volumes-to-exclude`` 指定した ``-volumes-to-exclude`` 場合 ``-shares-to-include`` は、がよりも優先されます ``-shares-to-include``。
- エクスポートポリシーをパラメータに指定し、エクスポートポリシーの親ボリュームをパラメータに指定した `-volumes-to-exclude`` 場合 ``-export-policies-to-include`` は、が ``-volumes-to-exclude`` よりも優先されます ``-export-policies-to-include``。
- 管理者はリストと `-file-extensions-to-exclude`` リストの両方を指定できます ``-file-extensions-to-include``。

``-file-extensions-to-exclude`` パラメータは、パラメータがチェックされる前にチェックされ ``-file-extensions-to-include`` ます。

FPolicyスコープの構成要素

次に示す使用可能なFPolicyスコープ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。



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。

情報の種類	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。	<code>-vserver vserver_name</code>
_ ポリシー名 _ スコープを関連付ける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。	<code>-policy-name policy_name</code>
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。	<code>-shares-to-include`</code> <code>`share_name`</code> はい。

<p><u>除外する共有</u></p> <p>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。</p>	<pre>-shares-to-exclude `share_name`はい。</pre>
<p>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。</p>	<pre>-volumes-to-include `volume_name`はい。</pre>
<p>除外するボリューム</p> <p>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。</p>	<pre>-volumes-to-exclude `volume_name`はい。</pre>
<p>ポリシーを含めるには <u> </u> をエクスポートします</p> <p>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。</p>	<pre>-export-policies-to-include `export_policy_name`はい。</pre>
<p>ポリシーを <u>exclude_ </u> にエクスポートします</p> <p>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。</p>	<pre>-export-policies-to-exclude `export_policy_name`はい。</pre>
<p><u>include </u> するファイル拡張子</p> <p>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。</p>	<pre>-file-extensions-to-include `file_extensions`はい。</pre>
<p><u> </u> ファイル拡張子を <u>exclude_ </u> に設定します</p> <p>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。</p>	<pre>-file-extensions-to-exclude `file_extensions`はい。</pre>
<p><u> </u> 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？ <u> </u></p> <p>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も適用するかどうかを指定します。このパラメータを <code>true</code> とすると、通常のファイルと同じ拡張子チェックがディレクトリオブジェクトに適用されます。このパラメータを <code>false</code> と、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くてもディレクトリに関する通知が送信されます。</p> <p>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 <code>true</code> に設定する必要があります</p>	<pre>-is-file-extension-check-on-directories-enabled{true</pre>
	<pre>false}</pre>

FPolicyスコープの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。

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。

情報の種類	必須	含める	自分の価値観
Storage Virtual Machine (SVM) 名	○	○	
ポリシー名	○	○	
対象に含める共有	いいえ		
共有を除外する	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		
対象から除外するエクスポートポリシー	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		

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。