SVMでのファイルの監視と管理にFPolicyを使用する

ONTAP 9

NetApp
December 20, 2024

目次

SVMでのファイルの監視と管理にFPolicyを使用する

FPolicyについて

FPolicyソリューションの2つの要素とは

FPolicyは、パートナーソリューションを通じてStorage Virtual Machine（SVM）上のファイルアクセスイベントの監視と管理に使用されるファイルアクセス通知フレームワークです。パートナーソリューションは、データガバナンスとコンプライアンス、ランサムウェア対策、データモビリティなど、さまざまなユースケースへの対応を支援します。

パートナーソリューションには、NetAppがサポートするサードパーティソリューションとNetApp製品のワークロードセキュリティとCloud Data Senseの両方が含まれます。

FPolicyソリューションには2つの要素があります。ONTAP FPolicyフレームワークは、クラスタでのアクティビティを管理し、パートナーアプリケーション（外部FPolicyサーバ）に通知を送信します。外部FPolicyサーバは、お客様のユースケースに対応するために、ONTAP FPolicyから送信された通知を処理します。

ONTAPフレームワークでは、FPolicyの設定の作成と管理、ファイルイベントの監視、および外部FPolicyサーバへの通知の送信を行います。ONTAP FPolicy は、外部 FPolicy サーバと Storage Virtual Machine （ SVM ）ノードの間の通信を可能にするインフラを提供します。

FPolicyフレームワークは、外部FPolicyサーバに接続し、クライアントアクセスの結果として特定のファイルシステムイベントが発生した場合にFPolicyサーバに通知を送信します。外部FPolicyサーバは、これらの通知を処理し、ノードに応答を送信します。通知処理の結果として実行される処理は、アプリケーション、およびノードと外部サーバの間の通信が非同期であるか同期であるかによって異なります。

同期通知および非同期通知とは

FPolicyは、FPolicyインターフェイスを介して外部FPolicyサーバに通知を送信します。通知は同期モードまたは非同期モードで送信されます。通知モードによって、FPolicyサーバに通知を送信したあとのONTAPの動作が決まります。

- * 非同期通知 *

  非同期通知では、ノードはFPolicyサーバからの応答を待たずに済むため、システムの全体的なスループットが向上します。このタイプの通知は、通知を評価した結果としてFPolicyサーバで処理する必要がないアプリケーションに適しています。たとえば、Storage Virtual Machine（SVM）管理者がファイルアクセスのアクティビティを監視および監査する場合などに使用します。

  FPolicyサーバが非同期モードで動作している場合にネットワークが停止すると、停止中に生成されたFPolicy通知がストレージノードに格納されます。FPolicyサーバがオンラインに戻ると、格納されている通知に関するアラートが通知され、ストレージノードから通知を取得できます。停止中に通知を保存できる期間は、最大10分まで設定できます。

  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永続的ストアを設定できます。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。

- * 同期通知 *

  同期モードで実行するように設定した場合、クライアント処理を続行するには、すべての通知をFPolicyサーバが確認応答する必要があります。このタイプの通知は、通知評価の結果に基づいてアクションが必要な場合に使用されます。たとえば、SVM管理者が要求を許可するか拒否するかを外部FPolicyサーバで指定された条件に基づいて判断する場合などに使用されます。

同期アプリケーションおよび非同期アプリケーション

FPolicyアプリケーションには、非同期と同期の両方でさまざまな用途があります。

非同期アプリケーションとは、ファイルやディレクトリへのアクセスやStorage Virtual Machine（SVM）上のデータが外部FPolicyサーバによって変更されないアプリケーションです。例：

- ファイルアクセスと監査ログ
- ストレージリソース管理

同期アプリケーションとは、データアクセスが変更されたり、外部FPolicyサーバによってデータが変更されたりするアプリケーションです。例：

- クォータの管理
- ファイルアクセスブロッキング
- ファイルのアーカイブと階層型ストレージ管理
- 暗号化サービスと復号化サービス
- 圧縮サービスと展開サービス

FPolicyの永続的ストア

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。ONTAP 9.14.1以降では、FPolicyの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。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。

この機能は、FPolicy外部モードでのみ使用できます。使用するパートナー アプリケーションが、この機能をサポートしている必要があります。パートナーと協力して、このFPolicy設定がサポートされていることを確認するようにしてください。

ONTAP 9.15.1以降では、FPolicyの永続的ストア設定が簡易化されています。 `persistent-store create`コマンドは、SVMのボリューム作成を自動化し、永続的ストアのベストプラクティスに従ってボリュームを設定します。

永続的ストアのベストプラクティスの詳細については、を参照してください"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"。

永続ストアの追加については、を参照してください"永続ストアの作成"。

FPolicy設定タイプ

FPolicyの基本設定には2つのタイプがあります。一方の設定では、外部FPolicyサーバを使用して通知の処理と対応を行います。もう一方の設定では外部FPolicyサーバを使用しません。代わりに、ONTAP内部のネイティブFPolicyサーバを使用して、拡張子に基づく単純なファイルブロッキングを行います。

- * 外部 FPolicy サーバ構成 *

  FPolicyサーバに通知が送信され、FPolicyサーバが要求をスクリーニングし、要求されたファイル操作をノードで許可するかどうかを決定するルールを適用します。同期ポリシーの場合、FPolicyサーバは要求されたファイル操作を許可またはブロックする応答をノードに送信します。

- * ネイティブ FPolicy サーバ構成 *

  通知は内部的にスクリーニングされます。要求は、FPolicyスコープで設定されているファイル拡張子に基づいて許可または拒否されます。

  *注：拒否されたファイル拡張子要求はログに記録されません。

ネイテイフ**FPolicy**セツテイヲサクセイスルシヨウコウ

ネイティブFPolicyの設定では、ONTAP内部のFPolicyエンジンを使用して、ファイルの拡張子に基づいてファイル操作を監視およびブロックします。このソリューションでは、外部FPolicyサーバ（FPolicyサーバ）は必要ありません。このシンプルなソリューションが必要な場合は、ネイティブファイルブロッキング構成を使用することをお勧めします。

ネイティブファイルブロッキングを使用すると、設定された処理およびフィルタリングイベントに一致するすべてのファイル操作を監視し、特定の拡張子を持つファイルへのアクセスを拒否できます。これがデフォルトの設定です。

この設定では、ファイルの拡張子のみに基づいてファイルへのアクセスをブロックすることができます。たとえば、拡張子を含むファイルをブロックするには `mp3`、拡張子がのファイルをターゲットとする特定の処理について通知を送信するようにポリシーを設定し `mp3`ます。このポリシーは、通知を生成する操作のファイル要求を拒否するように設定されて `mp3`います。

ネイティブFPolicy設定には次の事項が適用されます。

- FPolicyサーバベースのファイルスクリーニングでサポートされているフィルタとプロトコルのセットが、ネイティブファイルブロッキングでもサポートされます。
- ネイティブファイルブロッキングとFPolicyサーバベースファイルスクリーニングアプリケーションは同時に設定できます。

  そのためには、Storage Virtual Machine（SVM）に2つのFPolicyポリシーを設定します。1つはネイティブファイルブロッキング用に設定されたポリシー、もう1つはFPolicyサーバベースのファイルスクリーニング用に設定されたポリシーです。

- ネイティブファイルブロッキング機能は、ファイルの内容ではなく、拡張子に基づいてファイルをスクリーニングするだけです。

- シンボリックリンクの場合、ネイティブファイルブロッキングはルートファイルのファイル拡張子を使用します。

詳細については、をご覧ください "FPolicy：ネイティブファイルブロッキング"。

外部**FPolicy**サーバを使用する設定を作成する状況

通知の処理と管理に外部FPolicyサーバを使用するFPolicy設定は、ファイル拡張子に基づく単純なファイルブロッキング以上のことが必要なユースケースに、堅牢なソリューションを提供します。

ファイルアクセスイベントの監視と記録、クォータサービスの提供、単純なファイル拡張子以外の条件に基づくファイルブロッキングの実行、階層型ストレージ管理アプリケーションを使用したデータ移行サービスの提供、Storage Virtual Machine（SVM）のデータのサブセットのみを監視するきめ細かなポリシーセットの提供などを行う場合は、外部FPolicyサーバを使用する設定を作成する必要があります。

FPolicy実装でクラスタコンポーネントが果たす役割

FPolicyの実装では、クラスタ、それに含まれるStorage Virtual Machine（SVM）、およびデータLIFのすべてが役割を果たします。

- * クラスタ *

  クラスタにはFPolicyの管理フレームワークが含まれており、クラスタ内のすべてのFPolicyの設定に関する情報の保守と管理を行っています。

- * SVM *

  FPolicyの設定はSVMレベルで定義されます。設定の範囲はSVMで、SVMリソースに対してのみ機能します。あるSVMの設定で、別のSVMにあるデータに対するファイルアクセス要求を監視して通知を送信することはできません。

  FPolicyの設定は管理SVMで定義できます。管理SVMで定義した設定は、すべてのSVMで表示および使用できます。

- * データ LIF *

  FPolicyサーバへの接続は、FPolicyの設定が格納されたSVMに属するデータLIFを介して行われます。これらの接続に使用されるデータLIFは、通常のクライアントアクセスに使用されるデータLIFと同じ方法でフェイルオーバーできます。

FPolicyと外部FPolicyサーバの連携

Storage Virtual Machine（SVM）でFPolicyを設定して有効にすると、SVMに含まれているすべてのノードでFPolicyが実行されます。FPolicyは、外部FPolicyサーバ（FPolicyサーバ）との接続の確立と維持、通知の処理、およびFPolicyサーバとの間の通知メッセージの管理を行います。

また、接続管理の一環として、 FPolicy は次の役割を果たします。

- ファイル通知が正しいLIFを経由してFPolicyサーバに送信されるようにします。

- ポリシーに複数のFPolicyサーバが関連付けられている場合に、FPolicyサーバへの通知の送信時にロードバランシングが実行されるようにします。
- FPolicyサーバへの接続が切断された場合、接続の再確立が試行されます。
- 認証されたセッションを介してFPolicyサーバに通知を送信します。
- パススルーリードが有効になっている場合にクライアント要求を処理するためにFPolicyサーバによって確立されたパススルーリードデータ接続を管理します。

FPolicyツウシンニセイギョチャネルヲシヨウスルホウホウ

FPolicyは、Storage Virtual Machine（SVM）に含まれている各ノードのデータLIFから外部FPolicyサーバへの制御チャネル接続を開始します。FPolicyは制御チャネルを使用してファイル通知を送信するため、FPolicyサーバでは、SVMのトポロジに基づいて複数の制御チャネル接続が認識される場合があります。

ケンゲンツキツウシンテノデータアクセスチャネルノシヨウホウホウ

同期ユースケースでは、FPolicyサーバは権限付きデータアクセスパスを介してStorage Virtual Machine（SVM）上のデータにアクセスします。権限付きパスを介してアクセスすると、ファイルシステム全体がFPolicyサーバに公開されます。データファイルにアクセスして、情報の収集、ファイルのスキャン、ファイルの読み取り、ファイルへの書き込みを行うことができます。

外部FPolicyサーバが権限付きデータチャネルを介してSVMのルートからファイルシステム全体にアクセスできるため、権限付きデータチャネル接続はセキュアである必要があります。

権限付きデータアクセスチャネルでの**FPolicy**接続クレデンシャルの使用方法

FPolicyサーバは、FPolicy設定で保存されている特定のWindowsユーザクレデンシャルを使用して、クラスタノードへの権限付きデータアクセス接続を確立します。権限付きデータアクセスチャネル接続の確立用にサポートされているプロトコルはSMBだけです。

FPolicyサーバで権限付きデータアクセスが必要な場合は、次の条件を満たしている必要があります。

- クラスタでSMB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では、データチャネル接続を確立する際に、指定したWindowsユーザ名のクレデンシャルを使用します。データアクセスは、管理共有ONTAP _ ADMIN$を介して行われます。

ケンゲンツキデータアクセスヨウノスーパーユーザクレデンシャルノフヨトハ

ONTAPでは、FPolicy設定で設定されたIPアドレスとユーザクレデンシャルを組み合わせて、FPolicyサーバにスーパーユーザクレデンシャルを付与します。

スーパーユーザのステータスは、FPolicyサーバがデータにアクセスするときに次のPrivilegesに付与されます。

- 権限チェックの省略

  ユーザは、ファイルおよびディレクトリへのアクセスのチェックを回避します。

- 特殊ロックPrivileges

ONTAPは、ロックが設定されているかどうかに関係なく、すべてのファイルに対して読み取り、書き込み、変更アクセスを許可します。FPolicyサーバがファイルに対してバイト範囲ロックを取得すると、そのファイルに対する既存のロックがただちに削除されます。

- FPolicyチェックのバイパス

  アクセスではFPolicy通知は生成されません。

FPolicyによるポリシーの処理の管理方法

Storage Virtual Machine（SVM）には、優先度が異なる複数のFPolicyポリシーが割り当てられる場合があります。SVMで適切なFPolicyの設定を作成するには、FPolicyによるポリシーの処理の管理方法を理解しておくことが重要です。

各ファイルアクセス要求が最初に評価され、このイベントを監視しているポリシーが特定されます。監視対象イベントの場合は、関連するポリシーとともに監視対象イベントに関する情報が評価対象のFPolicyに渡されます。各ポリシーは、割り当てられた優先度の順に評価されます。

ポリシーを設定する際には、次の推奨事項を考慮する必要があります。

- ポリシーが常に他のポリシーよりも先に評価されるようにするには、そのポリシーの優先度を高く設定します。
- 監視対象イベントで要求されたファイルアクセス処理が成功することが、別のポリシーに照らして評価されるファイル要求の前提条件である場合は、最初のファイル処理の成功または失敗を制御するポリシーの優先度を高くします。

  たとえば、FPolicyのファイルのアーカイブおよびリストア機能を1つのポリシーで管理し、オンラインファイルでのファイルアクセス操作を2つ目のポリシーで管理している場合は、ファイルのリストアを管理するポリシーの優先度を高くしてから、2つ目のポリシーの管理操作を許可する必要があります。

- ファイルアクセス処理に適用される可能性のあるすべてのポリシーを評価する場合は、同期ポリシーの優先度を低くします。

既存のポリシーの優先度を変更するには、ポリシーのシーケンス番号を変更します。ただし、変更した優先順位に基づいてFPolicyでポリシーが評価されるようにするには、変更したシーケンス番号のポリシーを無効にしてから再度有効にする必要があります。

ノードと外部**FPolicy**サーバの間の通信プロセス

FPolicyの設定を適切に計画するには、ノードと外部FPolicyサーバの間の通信プロセスについて理解しておく必要があります。

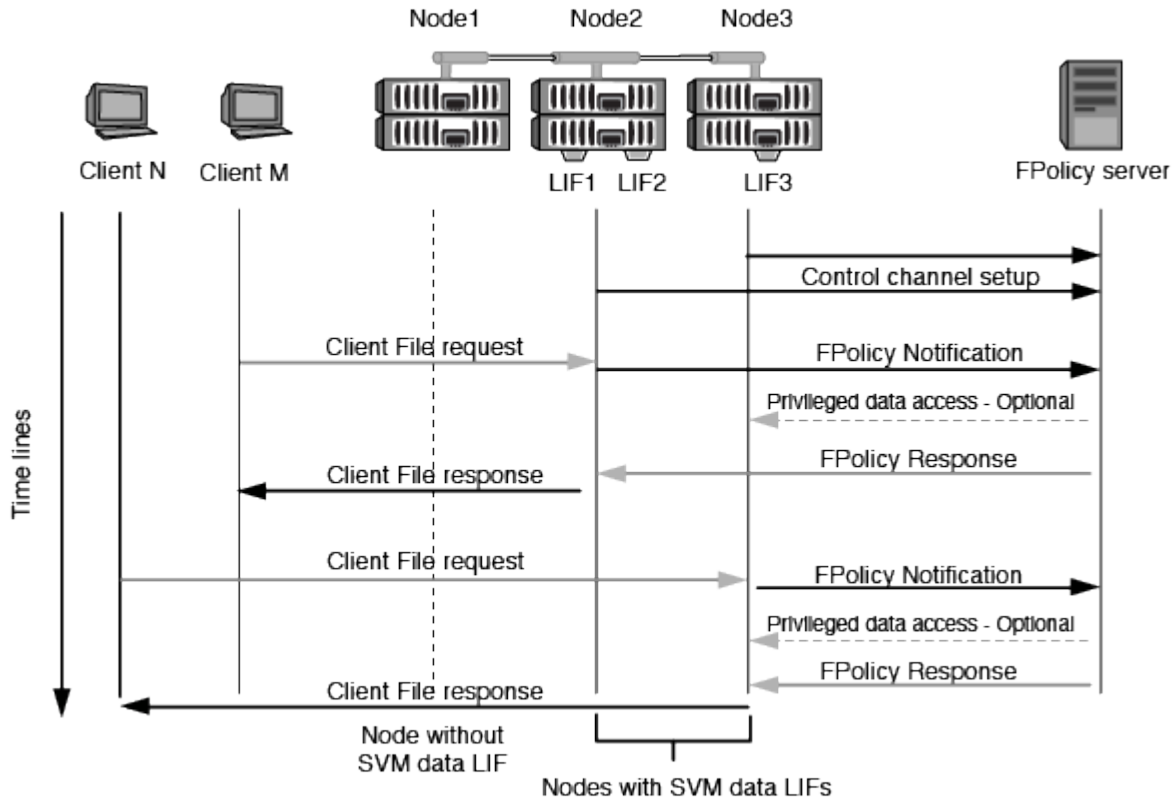
Storage Virtual Machine（SVM）に属しているすべてのノードは、TCP/IPを使用して外部FPolicyサーバへの接続を開始します。FPolicyサーバへの接続のセットアップには、ノードのデータLIFを使用します。そのため、接続のセットアップは、ノードでSVMのデータLIFが稼働している場合にのみ実行できます。

ポリシーが有効になっている場合、各ノードの各FPolicyプロセスでは、FPolicyサーバとの接続の確立が試行されます。ポリシー設定で指定されたFPolicy外部エンジンのIPアドレスとポートが使用されます。

この接続により、SVMに属する各ノードからFPolicyサーバへのデータLIFを介した制御チャネルが確立されます。さらに、データLIFのアドレスが同じノードでIPv4とIPv6の両方で設定されている場合、FPolicyはIPv4とIPv6の両方の接続の確立を試みます。したがって、SVMが複数のノードに展開されている場合、また

はIPv4アドレスとIPv6アドレスの両方が設定されている場合は、SVMでFPolicyポリシーを有効にしたあとに、クラスタからの複数の制御チャネルのセットアップ要求に対応する必要があります。

たとえば、クラスタに3つのノード（ノード1、ノード2、およびノード3）があり、SVMのデータLIFがノード2とノード3だけで設定されている場合、データボリュームの配置に関係なく、制御チャネルはノード2とノード3からのみ開始されます。ノード2にSVMに属するデータLIFが2つ（LIF1とLIF2）あり、最初にLIF1から接続を行うとします。FPolicyは、LIF1で障害が発生した場合、LIF2からの制御チャネルの確立を試みます。



LIFの移行時またはフェイルオーバー時の**FPolicy**による外部通信の管理方法

データLIFは、同じノードのデータポート、またはリモートノードのデータポートに移行できます。

データLIFがフェイルオーバーまたは移行されると、FPolicyサーバへの新しい制御チャネル接続が確立されます。その後、FPolicyはSMBクライアントおよびNFSクライアントのタイムアウトした要求を再試行でき、新しい通知が外部FPolicyサーバに送信されます。ノードは、SMBおよびNFSの元のタイムアウトした要求に対するFPolicyサーバの応答を拒否します。

ノードのフェイルオーバー時の**FPolicy**による外部通信の管理方法

FPolicy通信に使用されるデータポートをホストするクラスタノードで障害が発生すると、ONTAPはFPolicyサーバとノードの間の接続を切断します。

クラスタフェイルオーバーがFPolicyサーバに及ぼす影響は、FPolicy通信に使用されるデータポートを別のアクティブノードに移行するようにフェイルオーバーポリシーを設定することで軽減できます。移行が完了すると、新しいデータポートを使用して新しい接続が確立されます。

データポートを移行するようにフェイルオーバーポリシーが設定されていない場合、FPolicyサーバは障害が発生したノードが稼働するまで待機する必要があります。ノードが稼働すると、そのノードから新しいSession IDを使用して新しい接続が開始されます。

FPolicyサーバは、切断された接続をキープアライブプロトコルメッセージで検出します。Session IDをパージするタイムアウトは、FPolicyの設定時に決定されます。デフォルトのキープアライブタイムアウトは2分です。

SVMネームスペースにおけるFPolicyサービスの仕組み

ONTAP は、統合 Storage Virtual Machine （ SVM ）ネームスペースを提供します。ジャンクションによってクラスタ全体のボリュームを統合し、単一の論理ファイルシステムを実現します。FPolicy サーバはネームスペーストポロジを認識し、ネームスペース全体に FPolicy サービスを提供します。

ネームスペースは SVM に固有のもので、その内部に含まれています。したがって、ネームスペースは SVM コンテキストからのみ表示できます。ネームスペースには次のような特徴があります。

- 各 SVM には単一のネームスペースが存在します。ネームスペースのルートはルートボリュームで、ネームスペース内ではスラッシュ（ / ）で表されます。
- それ以外のボリュームには、ルート（ / ）より下のジャンクションポイントがあります。
- ボリュームジャンクションは、クライアントに対して透過的です。
- 単一の NFS エクスポートは、ネームスペース全体へのアクセスを提供できます。あるいは、エクスポートポリシーで特定のボリュームをエクスポートできます。
- ネームスペース内のボリューム、ボリューム内の qtree 、またはディレクトリに SMB 共有を作成できます。
- ネームスペースアーキテクチャは柔軟です。

  一般的なネームスペースアーキテクチャの例を次に示します。

  - ルートからの分岐が 1 つだけのネームスペース
  - ルートからの分岐が複数あるネームスペース
  - ルートから分岐していないボリュームが複数あるネームスペース

FPolicyパススルーリードによる階層型ストレージ管理のユーザビリティの向上

パススルーリードを使用すると、オフラインファイルに対する読み取りアクセスを（階層型ストレージ管理（HSM）サーバとして機能している）FPolicyサーバから提供できます。セカンダリストレージシステムからプライマリストレージシステムにファイルをリコールする必要はありません。

SMBサーバ上にあるファイルにHSMを提供するようにFPolicyサーバが設定されている場合、ポリシーベースのファイル移行が実行されます。この場合、ファイルはセカンダリストレージにオフラインで保存され、スタブファイルのみがプライマリストレージに残ります。スタブファイルはクライアントからは通常のファイルとして認識されますが、実際には元のファイルと同じサイズのスパースファイルです。スパースファイルにはSMBオフラインビットが設定されており、セカンダリストレージに移行された実際のファイルを参照しています。

通常、オフラインファイルの読み取り要求を受信した場合は、要求されたコンテンツをプライマリストレージにリコールしてから、プライマリストレージ経由でアクセスする必要があります。データをプライマリストレ

ージにリコールする必要があるため、望ましくない影響がいくつかあります。望ましくない影響としては、コンテンツをリコールしてから要求に応答する必要があることが原因でクライアント要求に対するレイテンシが増加したり、プライマリストレージでリコールされるファイルに必要なスペースが増加したりすることがあります。

FPolicyパススルーリードを使用すると、移行されたオフラインファイルに対する読み取りアクセスをHSMサーバ（FPolicyサーバ）が提供できます。セカンダリストレージシステムからプライマリストレージシステムにファイルをリコールする必要はありません。プライマリストレージにファイルをリコールする代わりに、読み取り要求をセカンダリストレージから直接処理できます。

FPolicyのパススルーリード処理では、コピーオフロード（ODX）はサポートされません。

パススルーリードには次のような利点があり、ユーザビリティが向上します。

- 要求されたデータをリコールするための十分なスペースがプライマリストレージにない場合でも、読み取り要求を処理できます。
- スクリプトやバックアップソリューションで多数のオフラインファイルにアクセスする必要がある場合など、データリコールが急増する可能性がある場合は、容量とパフォーマンスの管理が向上します。
- Snapshotコピー内のオフラインファイルに対する読み取り要求を処理できます。

  Snapshotコピーは読み取り専用であるため、スタブファイルがSnapshotコピー内にある場合、FPolicyサーバは元のファイルをリストアできません。パススルーリードを使用すると、この問題が解消されます。

- 読み取り要求をセカンダリストレージ上のファイルにアクセスして処理するタイミングと、オフラインファイルをプライマリストレージにリコールするタイミングを制御するポリシーを設定できます。

  たとえば、オフラインファイルがプライマリストレージに移行されるまでに、指定した期間内にオフラインファイルにアクセスできる回数を指定するポリシーをHSMサーバ上に作成できます。このタイプのポリシーにより、滅多にアクセスされないファイルのリコールを回避できます。

FPolicyパススルーリードが有効になっている場合の読み取り要求の管理方法

Storage Virtual Machine（SVM）とFPolicyサーバ間の接続を最適な形で設定できるように、FPolicyパススルーリードが有効になっている場合の読み取り要求の管理方法を理解しておく必要があります。

FPolicyパススルーリードが有効になっている場合にSVMがオフラインのファイルに対する要求を受信すると、FPolicyは標準の接続チャネルを介してFPolicyサーバ（HSMサーバ）に通知を送信します。

通知を受信すると、FPolicyサーバは通知で送信されたファイルパスからデータを読み取り、要求されたデータをSVMとFPolicyサーバの間に確立されたパススルーリード権限付きデータ接続を介してSVMに送信します。

データが送信されると、FPolicyサーバは読み取り要求にallowまたはdenyとして応答します。読み取り要求が許可されたか拒否されたかに基づいて、ONTAPは要求された情報またはエラーメッセージをクライアントに送信します。

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。

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ままです。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 `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、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えます。

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。
   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`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
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

カウンタ	説明
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		

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
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。 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。	-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。 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`フアイルヨミトリソウサ • `write`フア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 _ 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。	`-filters` `filter`はい。

30 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。

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。 • Failures due to NTFS permissions. • Failures due to Unix mode bits. • Failures due to NFSv4 ACLs.
`-monitor-fileop-failure{true`	`false}`

- 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。

FPolicy + SMB [illegible] ィルタノクミアワセ

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

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`	○	なし
_ ポリシー名 _ FPolicyポリシーの名前を指定します。 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`	○	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で区切って指定します。 • 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。	○	なし

永続ストア 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。	`-persistent -store persistent_store_name`	いいえ	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。	`-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。 • 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。	`-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。 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る必要があり、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`cifs`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}

×（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に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。 • 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。	-privileged-user-name user_name

×（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。 • 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。 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。 • 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。 パススルーリー	`-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に 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。デフォルト値はで `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に設定されている `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をに `true`設定する必要があり `-is-file-extension-check-on-directories-enabled parameter`ます。

このパラメータをに設定する `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	○	
ポリシー名	○	
イベント名	○	
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		

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。	`-vserver vserver_name`
_ 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。	`-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も適用するかどうかを指定します。このパラメータをに設定 `true`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。このパラメータをに設定する `false`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。 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		

FPolicy設定の作成

FPolicy外部エンジンの作成

FPolicy設定の作成を開始するには、外部エンジンを作成する必要があります。外部エンジンは、FPolicyが外部FPolicyサーバへの接続を確立および管理する方法を定義します。内部のONTAPエンジン（標準の外部エンジン）を単純なファイルブロッキングに使用している設定の場合は、FPolicy外部エンジンを別途設定する必要はなく、この手順を実行する必要もありません。

必要なもの

"外部エンジン"ワークシートを完成させる必要があります。

タスクの内容

外部エンジンがMetroCluster設定で使用されている場合は、ソースサイトで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。

手順

1. コマンドを使用してFPolicy外部エンジンを作成し `vserver fpolicy policy external-engine create`ます。

   次のコマンドは、Storage Virtual Machine（SVM）vs1.example.com上に外部エンジンを作成します。FPolicyサーバとの外部通信に認証は必要ありません。

   ```
   vserver fpolicy policy external-engine create -vserver-name vs1.example.com
   -engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
   no-auth
   ```

2. コマンドを使用してFPolicy外部エンジンの設定を確認します `vserver fpolicy policy external-engine show`。

   次のコマンドは、SVM vs1.example.comで設定されているすべての外部エンジンに関する情報を表示します。

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com
   ```

   ```
                                Primary        Secondary
   External
   Vserver             Engine   Servers        Servers       Port Engine
   Type
   ----------------    ---------- -------------- ----------- ------
   -----------
   vs1.example.com     engine1    10.1.1.2,      -             6789
   synchronous
                                  10.1.1.3
   ```

   次のコマンドは、 SVM vs1.example.com 上の「 engine1 」という外部エンジンに関する詳細情報を表示します。

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
   -name engine1
   ```

```
                                Vserver: vs1.example.com
                                 Engine: engine1
              Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
       Port Number of FPolicy Service: 6789
            Secondary FPolicy Servers: -
                 External Engine Type: synchronous
SSL Option for External Communication: no-auth
           FQDN or Custom Common Name: -
         Serial Number of Certificate: -
               Certificate Authority: -
```

FPolicyイベントの作成

FPolicyポリシーの設定を作成する手順の一環として、FPolicyイベントを作成する必要があります。FPolicyポリシーの作成時にイベントを関連付けます。イベントは、監視するプロトコルと、監視およびフィルタリングするファイルアクセスイベントを定義します。

開始する前に

FPolicyイベントを完了する必要があります"ワークシート"。

FPolicyイベントの作成

1. コマンドを使用してFPolicyイベントを作成し `vserver fpolicy policy event create`ます。

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -file-operations open,close,read,write
   ```

2. コマンドを使用してFPolicyイベントの設定を確認します `vserver fpolicy policy event show`。

   ```
   vserver fpolicy policy event show -vserver vs1.example.com
   ```

   ```
                    Event                File                      Is Volume
   Vserver          Name      Protocols  Operations    Filters     Operation
   ---------------  --------- ---------  ------------- ---------
   ------------
   vs1.example.com  event1    cifs       open, close,  -           false
                                         read, write
   ```

FPolicyアクセス拒否イベントを作成する

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。

1. コマンドを使用してFPolicyイベントを作成し `vserver fpolicy policy event create`ます。

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name
event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

FPolicy永続的ストアの作成

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。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。

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。

永続ストアを作成するには、ONTAPのリリースに応じて次の2つの方法があります。

- ONTAP 9.15.1以降：永続ストアを作成すると、ONTAPでボリュームが自動的に作成されて設定されます。これにより、FPolicyの永続的ストアの設定が簡素化され、すべてのベストプラクティスが実装されます。
- ONTAP 9.14.1：ボリュームを手動で作成して設定し、新しく作成したボリューム用の永続的ストアを作成します。

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。

永続ストアの作成（**ONTAP 9 .15.1**以降）

開始する前に

- 永続的ストアを作成するSVMには、アグリゲートが少なくとも1つ必要です。
- SVMで使用可能なアグリゲートへのアクセスと、ボリュームを作成するための十分な権限が必要です。

手順

1. 永続的ストアを作成します。これにより、ボリュームが自動的に作成および設定されます。

```
vserver fpolicy persistent-store create -vserver <vserver> -persistent-store
<name> -volume <volume_name> -size <size> -autosize-mode
<off|grow|grow_shrink>
```

   - `vserver`パラメータは、SVMの名前です。
   - `persistent-store`パラメータは、永続ストアの名前です。
   - `volume`パラメータは、永続的ストアボリュームの名前です。

     既存の空のボリュームを使用する場合は、コマンドを使用してボリューム `volume show`を検索し、volumeパラメータで指定します。

   - この `size`パラメータは、外部サーバ（パートナーアプリケーション）に配信されないイベントを保持する期間に基づいています。

たとえば、1秒あたり30Kの通知があるクラスタで30分間のイベントを維持する場合は、次のコマンドを実行します。

必要なボリュームサイズ= 30000 x 30 x 60 x 0.6KB（通知レコードの平均サイズ）= 32400000 KB =~32GB

おおよその通知速度を確認するには、FPolicyパートナーアプリケーションに連絡するか、FPolicyカウンタを利用します `requests_dispatched_rate`。

> 既存のボリュームを使用する場合、sizeパラメータはオプションです。sizeパラメータに値を指定すると、指定したサイズに一致するボリュームが変更されます。

- パラメータは `autosize-mode`、ボリュームのオートサイズモードを指定します。サポートされるオートサイズモードは次のとおりです。
  - off -使用済みスペースの量に応じてボリュームのサイズが拡張または縮小されません。
  - grow -ボリュームの使用済みスペースが拡張しきい値を超えると、ボリュームは自動的に拡張されます。
  - grow_shrink -使用済みスペースの量に応じてボリュームのサイズが拡張または縮小されます。

2. FPolicyポリシーを作成し、そのポリシーに永続ストア名を追加します。詳細については、を参照してください "FPolicyポリシーを作成する"。

永続ストアの作成（**ONTAP 9 .14.1**）

ボリュームを作成し、そのボリュームを使用する永続的ストアを作成できます。作成したボリュームを外部ユーザプロトコルアクセス（CIFS / NFS）からブロックできます。

手順

1. 永続ストア用にプロビジョニング可能な空のボリュームをSVMに作成します。

```
volume create -vserver <SVM Name> -volume <volume> -state <online> -policy
<default> -unix-permissions <777> -size <value> -aggregate <aggregate name>
-snapshot-policy <none>
```

十分なRBAC Privileges（ボリュームの作成）を持つ管理者ユーザは、必要なサイズのボリュームを（volume CLIコマンドまたはREST APIを使用して）作成し、永続的ストアのcreate CLIコマンドまたはREST APIでとしてボリュームの名前を指定する必要があります `-volume`。

- `vserver`パラメータは、SVMの名前です。
- `volume`パラメータは、永続的ストアボリュームの名前です。
- ボリュームを使用できるようにするには、 `state`パラメータをonlineに設定する必要があります。
- `policy`FPolicyサービスポリシーをすでに設定している場合、パラメータはに設定されます。そうでない場合は、あとでコマンドを使用してポリシーを追加できます `volume modify`。
- `unix-permissions`パラメータはオプションです。
- この `size`パラメータは、外部サーバ（パートナーアプリケーション）に配信されないイベントを保持する期間に基づいています。

  たとえば、1秒あたり30Kの通知があるクラスタで30分間のイベントを維持する場合は、次のコマンド

を実行します。

必要なボリュームサイズ= 30000 x 30 x 60 x 0.6KB（通知レコードの平均サイズ）= 32400000 KB =~32GB

おおよその通知速度を確認するには、FPolicyパートナーアプリケーションに連絡するか、FPolicyカウンタを利用します `requests_dispatched_rate`。

- FlexVolボリュームの場合はaggregateパラメータが必要です。それ以外の場合は必須ではありません。
- `snapshot-policy`パラメータはnoneに設定する必要があります。これにより、スナップショット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くなり、イベント処理の重複を防ぐことができます。

既存の空のボリュームを使用する場合は、コマンドを使用してボリュームを検索し、コマンドを使用し `volume show`て必要な変更を行います。 `volume modify`永続ストアのポリシー、サイズ、およびパラメータが正しく設定されていることを確認します `snapshot-policy`。

2. 永続ストアを作成します。

```
vserver fpolicy persistent store create -vserver <SVM> -persistent-store
<PS_name> -volume <volume>
```

- `vserver`パラメータは、SVMの名前です。
- `persistent-store`パラメータは、永続ストアの名前です。
- `volume`パラメータは、永続的ストアボリュームの名前です。

3. FPolicyポリシーを作成し、そのポリシーに永続ストア名を追加します。詳細については、を参照してください "FPolicyポリシーを作成する"。

FPolicyポリシーを作成する

FPolicyポリシーを作成するときは、外部エンジンと1つ以上のイベントをポリシーに関連付けます。また、このポリシーでは、必須のスクリーニングが必要かどうか、FPolicyサーバにStorage Virtual Machine（SVM）上のデータへの権限付きアクセスが許可されているかどうか、オフラインファイルのパススルーリードが有効かどうかを指定します。

必要なもの

- FPolicyポリシーワークシートを完成させる必要があります。
- FPolicyサーバを使用するようにポリシーを設定する場合は、外部エンジンが存在している必要があります。
- FPolicyポリシーに関連付けるFPolicyイベントが少なくとも1つ存在している必要があります。
- 権限付きデータアクセスを設定する場合は、SVM上にSMBサーバが存在している必要があります。
- ポリシーの永続ストアを設定するには、エンジンタイプを* async にし、ポリシーを non-mandatory *にする必要があります。

詳細については、を参照してください "永続ストアの作成"。

手順

1. FPolicyポリシーを作成します。

```
vserver fpolicy policy create -vserver-name vserver_name -policy-name
policy_name -engine engine_name -events event_name, [-persistent-store
PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
privileged-user-name domain\user_name] [-is-passthrough-read-enabled
{true|false}]
```

   - FPolicy ポリシーには 1 つ以上のイベントを追加できます。
   - デフォルトでは、必須のスクリーニングが有効になっています。
   - パラメータをに `yes`設定して権限付きアクセスを許可する場合 `-allow-privileged-access`は、権限付きアクセスの権限付きユーザ名も設定する必要があります。
   - パラメータをに `true`設定してパススルーリードを設定する場合 `-is-passthrough-read-enabled`は、権限付きデータアクセスも設定する必要があります。

     次のコマンドは、 "event1" というイベントと、 "engine1" という外部エンジンが関連付けられた "policy1 " という名前のポリシーを作成します。このポリシーでは、ポリシー設定にデフォルト値を使用します。 `vserver fpolicy policy create -vserver vs1.example.com -policy -name policy1 -events event1 -engine engine1`

     次のコマンドは、 "event2`" というイベントと、 "engine2`" という外部エンジンが関連付けられた "policy2`" というポリシーを作成します。このポリシーは、指定したユーザ名を使用して権限付きアクセスを使用するように設定されています。パススルーリードが有効になっている場合：

     ```
     vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
     -events event2 -engine engine2 -allow-privileged-access yes -privileged-
     user-name example\archive_acct -is-passthrough-read-enabled true
     ```

     次のコマンドは ' event3` というイベントが関連付けられた ' ' native1` という名前のポリシーを作成しますこのポリシーでは標準のエンジンを使用し、デフォルト値をポリシー設定に使用します。

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

2. コマンドを使用してFPolicyポリシーの設定を確認します `vserver fpolicy policy show`。

   次のコマンドは、次の情報を含む、設定された3つのFPolicyポリシーに関する情報を表示します。

   - ポリシーに関連付けられている SVM
   - ポリシーに関連付けられている外部エンジン
   - ポリシーに関連付けられているイベント
   - スクリーニングを必須にするかどうか
   - 権限付きアクセスが必要かどうか `vserver fpolicy policy show`

```
   Vserver       Policy     Events    Engine    Is Mandatory  Privileged
                 Name                                         Access
--------------   ---------  --------- --------- ------------
-----------
vs1.example.com  policy1    event1    engine1   true          no
vs1.example.com  policy2    event2    engine2   true          yes
vs1.example.com  native1    event3    native    true          no
```

FPolicyスコープを作成する

FPolicy ポリシーを作成したら、 FPolicy スコープを作成する必要があります。スコープを作成するときに、スコープを FPolicy ポリシーに関連付けます。スコープは、FPolicy ポリシーが適用される範囲を定義します。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に基づいて、対象とするファイルまたは除外するファイルを指定できます。

必要なもの

FPolicy スコープワークシートを完成させる必要があります。FPolicy ポリシーには、関連付けられた外部エンジンが存在する必要があり（外部 FPolicy サーバを使用するようにポリシーを設定する場合）、 FPolicy イベントを少なくとも 1 つは関連付ける必要があります。

手順

1. コマンドを使用してFPolicyスコープを作成し `vserver fpolicy policy scope create`ます。

   ```
   vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name
   policy1 -volumes-to-include datavol1,datavol2
   ```

2. コマンドを使用してFPolicyスコープの設定を確認します `vserver fpolicy policy scope show`。

   ```
   vserver fpolicy policy scope show -vserver vs1.example.com -instance
   ```

```
                    Vserver: vs1.example.com
                     Policy: policy1
          Shares to Include: -
          Shares to Exclude: -
         Volumes to Include: datavol1, datavol2
         Volumes to Exclude: -
 Export Policies to Include: -
 Export Policies to Exclude: -
 File Extensions to Include: -
 File Extensions to Exclude: -
```

FPolicyポリシーを有効にする

FPolicy ポリシーの設定が完了したら、 FPolicy ポリシーを有効にします。ポリシーを有効にすると、優先度が設定され、ポリシーのファイルアクセスの監視が開始されます。

必要なもの

FPolicy ポリシーには、関連付けられた外部エンジンが存在する必要があり（外部 FPolicy サーバを使用するようにポリシーを設定する場合）、 FPolicy イベントを少なくとも 1 つは関連付ける必要があります。FPolicy ポリシースコープが存在し、 FPolicy ポリシーに割り当てられている必要があります。

タスクの内容

Storage Virtual Machine（SVM）で複数のポリシーを有効にし、複数のポリシーを同じファイルアクセスイベントに登録している場合は、優先度が使用されます。標準のエンジン設定を使用するポリシーは、ポリシーを有効にするときに割り当てられたシーケンス番号に関係なく、他のエンジンのポリシーよりも優先度が高くなります。

管理 SVM ではポリシーを有効にできません。

手順

1. コマンドを使用して、FPolicyポリシーを有効にし `vserver fpolicy enable`ます。

   ```
   vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
   -sequence-number 1
   ```

2. コマンドを使用して、FPolicyポリシーが有効になっていることを確認します `vserver fpolicy show`。

   ```
   vserver fpolicy show -vserver vs1.example.com
   ```

   ```
                                    Sequence
   Vserver           Policy Name      Number  Status   Engine
   ---------------  ----------------- --------  -------- ---------
   vs1.example.com  policy1                 1  on       engine1
   ```

FPolicy設定を管理します。

FPolicyの設定変更

FPolicy設定の変更用コマンド

FPolicyの設定を変更するには、設定を構成する要素を変更します。外部エンジン、FPolicyイベント、FPolicyスコープ、FPolicy永続ストア、およびFPolicyポリシーを変更できます。FPolicyポリシーを有効または無効にすることもできます。FPolicyポリシーを無効にすると、そのポリシーのファイル監視が中止されます。

設定を変更する前に、FPolicyポリシーを無効にする必要があります。

変更する項目	使用するコマンド
外部エンジン	`vserver fpolicy policy external-engine modify`
イベント	`vserver fpolicy policy event modify`
スコープ	`vserver fpolicy policy scope modify`
永続的ストア	`vserver fpolicy persistent-store modify`
ポリシー	`vserver fpolicy policy modify`

詳細については、各コマンドのマニュアル ページを参照してください。

FPolicyポリシーを有効または無効にする

設定の完了後にFPolicyポリシーを有効にできます。ポリシーを有効にすると、優先度が設定され、ポリシーのファイルアクセスの監視が開始されます。ポリシーのファイルアクセスの監視を停止するには、FPolicyポリシーを無効にします。

必要なもの

FPolicyポリシーを有効にする前に、FPolicyの設定を完了しておく必要があります。

タスクの内容

- Storage Virtual Machine（SVM）で複数のポリシーを有効にし、複数のポリシーを同じファイルアクセスイベントに登録している場合は、優先度が使用されます。
- 標準のエンジン設定を使用するポリシーは、ポリシーを有効にするときに割り当てられたシーケンス番号に関係なく、他のエンジンのポリシーよりも優先度が高くなります。
- FPolicyポリシーの優先度を変更する場合は、ポリシーを無効にしてから、新しいシーケンス番号を使用して再度有効にする必要があります。

ステップ

1. 適切な操作を実行します。

状況	入力するコマンド
FPolicyポリシーを有効にする	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`
FPolicyポリシーを無効にする	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

FPolicy設定に関する情報を表示する

showコマンドの機能

コマンドの仕組みを理解しておくと、FPolicyの設定に関する情報を表示するときに役立ち `show`ます。

パラメータを追加せずにコマンドを実行すると、 `show`情報が要約形式で表示されます。また `show`、各コマンドには、同じ2つのオプションパラメータ、およびが `-fields`あり `-instance`ます。

コマンドでパラメータを `show`使用する `-instance`と、コマンド出力には詳細情報がリスト形式で表示されます。場合によっては、詳細な出力に時間がかかり、必要以上の情報が含まれることがあります。パラメータを使用すると、指定したフィールドの情報のみが表示されるように出力をカスタマイズできます `-fields fieldname[,fieldname…]`。指定できるフィールドを特定するには、パラメータのあと `-fields`にと入力します `?`。

> パラメータを指定したコマンドの `-fields`出力には `show`、要求したフィールドに関連する他の関連フィールドや必要なフィールドが表示される場合があります。

すべて `show`のコマンドには、その出力をフィルタリングして、コマンド出力に表示される情報の範囲を絞り込むことができる1つ以上のオプションパラメータがあります。コマンドで使用可能なオプションパラメータを確認するには、コマンドのあとに `show`と入力し `?`ます。

`show`コマンドでは、UNIX形式のパターンおよびワイルドカードがサポートされ、コマンドパラメータ引数の複数の値を照合できます。たとえば、ワイルドカード演算子（ `*` ）、 `NOT` 演算子（ `!` ）、 `OR` 演算子（ `|` ）、範囲演算子（ `integer...integer` ）、 `less-than` 演算子（ `<` ）、 `greater-than` 演算子（ `>` ）、 `less-than-or-equal-to` 演算子（ `\<=` ）、 `greater-than-or-equal-to` 演算子（ `>=` ）を指定する場合に使用できます。

UNIX形式のパターンおよびワイルドカードの使用の詳細については、を参照してくださいONTAPコマンドラインインターフェイスの使用。

FPolicy設定に関する情報を表示するコマンド

FPolicy外部エンジン、イベント、スコープ、およびポリシーに関する情報など、FPolicyの設定に関する情報を表示するには、コマンドを使用し `fpolicy show`ます。

FPolicy に関する情報の表示	使用するコマンド
外部エンジン	`vserver fpolicy policy external-engine show`
イベント	`vserver fpolicy policy event show`
スコープ	`vserver fpolicy policy scope show`
ポリシー	`vserver fpolicy policy show`

詳細については、各コマンドのマニュアル ページを参照してください。

FPolicyポリシーのステータスに関する情報を表示する

FPolicyポリシーのステータスに関する情報を表示して、ポリシーが有効になっているかどうか、使用するように設定されている外部エンジン、ポリシーのシーケンス番号、およびFPolicyポリシーが関連付けられているStorage Virtual Machine（SVM）を確認できます。

タスクの内容

いずれのパラメータも指定しない場合、次の情報が表示されます。

- SVM名
- ポリシー名
- ポリシーのシーケンス番号
- ポリシーのステータス

クラスタまたは特定のSVMで設定されているFPolicyポリシーのステータスに関する情報の表示に加え、コマンドパラメータを使用して、他の条件によってコマンドの出力をフィルタリングすることができます。

パラメータを指定すると、リストされているポリシーに関する詳細情報を表示できます `-instance`。また、パラメータを使用して、指定したフィールドのみをコマンド出力に表示したり、使用できるフィールドを確認したり `-fields ?`することもできます `-fields`。

ステップ

1. 適切なコマンドを使用して、FPolicyポリシーのステータスに関する情報をフィルタリングして表示します。

ステータス情報を表示するポリシー	入力するコマンド
クラスタのポリシー	`vserver fpolicy show`
指定したステータスのポリシー	`vserver fpolicy show -status {on
off}`	指定したSVMのポリシー
`vserver fpolicy show -vserver vserver_name`	指定したポリシー名のポリシー
`vserver fpolicy show -policy-name policy_name`	指定した外部エンジンを使用するポリシー

例

次の例は、クラスタのFPolicyポリシーに関する情報を表示します。

```
cluster1::> vserver fpolicy show
                                          Sequence
Vserver              Policy Name           Number  Status      Engine
-------------------- -------------------- --------  ---------   ---------
FPolicy              cserver_policy       -         off         eng1
vs1.example.com      v1p1                 -         off         eng2
vs1.example.com      v1p2                 -         off         native
vs1.example.com      v1p3                 -         off         native
vs1.example.com      cserver_policy       -         off         eng1
vs2.example.com      v1p1                 3         on          native
vs2.example.com      v1p2                 1         on          eng3
vs2.example.com      cserver_policy       2         on          eng1
```

有効な**FPolicy**ポリシーに関する情報を表示する

有効なFPolicyポリシーに関する情報を表示して、使用するように設定されている外部エンジン、ポリシーの優先度、およびFPolicyポリシーが関連付けられているStorage Virtual Machine（SVM）を確認できます。

タスクの内容

いずれのパラメータも指定しない場合、次の情報が表示されます。

- SVM名
- ポリシー名
- ポリシーの優先度

コマンドパラメータを使用すると、指定した条件でコマンドの出力をフィルタリングできます。

ステップ

1. 適切なコマンドを使用して、有効なFPolicyポリシーに関する情報を表示します。

情報を表示する有効なポリシー	入力するコマンド
クラスタのポリシー	`vserver fpolicy show-enabled`
指定したSVMのポリシー	`vserver fpolicy show-enabled -vserver vserver_name`
指定したポリシー名のポリシー	`vserver fpolicy show-enabled -policy-name policy_name`
指定したシーケンス番号のファイル	`vserver fpolicy show-enabled -priority integer`

例

次の例は、クラスタの有効なFPolicyポリシーに関する情報を表示します。

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

FPolicyサーバの接続を管理します。

外部FPolicyサーバへの接続

接続がすでに終了している場合は、ファイル処理を有効にするために、外部FPolicyサーバへの手動接続が必要になることがあります。サーバのタイムアウトに達した後、または何らかのエラーが原因で接続が終了します。または、管理者が接続を手動で終了することもできます。

タスクの内容

致命的なエラーが発生すると、FPolicyサーバへの接続が終了する可能性があります。致命的なエラーの原因となった問題を解決したら、FPolicyサーバに手動で再接続する必要があります。

手順

1. コマンドを使用して外部FPolicyサーバに接続します `vserver fpolicy engine-connect`。

   コマンドの詳細については、マニュアルページを参照してください。

2. コマンドを使用して、外部FPolicyサーバが接続されていることを確認します `vserver fpolicy show-engine`。

   コマンドの詳細については、マニュアルページを参照してください。

外部FPolicyサーバからの切断

外部FPolicyサーバからの手動での切断が必要になる場合があります。これは、FPolicyサーバで通知要求の処理に関する問題が発生した場合や、FPolicyサーバでメンテナンスを実施する必要がある場合に適しています。

手順

1. コマンドを使用して、外部FPolicyサーバから切断し `vserver fpolicy engine-disconnect`ます。

   コマンドの詳細については、マニュアルページを参照してください。

2. コマンドを使用して、外部FPolicyサーバが切断されたことを確認します `vserver fpolicy show-engine`。

コマンドの詳細については、マニュアルページを参照してください。

外部**FPolicy**サーバへの接続に関する情報を表示する

クラスタまたは指定したStorage Virtual Machine（SVM）の外部FPolicyサーバ（FPolicyサーバ）への接続に関するステータス情報を表示できます。この情報は、接続されているFPolicyサーバを確認するのに役立ちます。

タスクの内容

いずれのパラメータも指定しない場合、次の情報が表示されます。

- SVM名
- ノード名
- FPolicyポリシー名
- FPolicyサーバのIPアドレス
- FPolicyサーバノステータス
- FPolicyサーバのタイプ

クラスタまたは特定のSVMのFPolicy接続に関する情報の表示に加え、コマンドパラメータを使用して、他の条件によってコマンドの出力をフィルタリングすることができます。

パラメータを指定すると、リストされているポリシーに関する詳細情報を表示できます `-instance`。また、パラメータを使用して、指定したフィールドのみをコマンド出力に表示することもできます `-fields`。パラメータのあとに `-fields`と入力すると、使用できるフィールドを確認できます `?`。

ステップ

1. 適切なコマンドを使用して、ノードとFPolicyサーバの間の接続ステータスに関する情報をフィルタリングして表示します。

接続ステータス情報を表示するFPolicy サーバ	入力するコマンド
指定したもの	`vserver fpolicy show-engine -server IP_address`
指定したSVMのもの	`vserver fpolicy show-engine -vserver vserver_name`
指定したポリシーに関連付けられているポリシー	`vserver fpolicy show-engine -policy-name policy_name`

指定したサーバステータスのファイル	`vserver fpolicy show-engine -server-status status` サーバのステータスは、次のいずれかになります。 • `connected` • `disconnected` • `connecting` • `disconnecting`
指定したタイプのファイル	`vserver fpolicy show-engine -server-type type` FPolicyサーバのタイプは次のいずれかになります。 • `primary` • `secondary`
指定した理由で切断されたもの	`vserver fpolicy show-engine -disconnect-reason text` 切断の理由はさまざまです。切断の一般的な理由は次のとおりです。 • `Disconnect command received from CLI.` • `Error encountered while parsing notification response from FPolicy server.` • `FPolicy Handshake failed.` • `SSL handshake failed.` • `TCP Connection to FPolicy server failed.` • `The screen response message received from the FPolicy server is not valid.`

例

次の例は、SVM vs1.example.com上のFPolicyサーバへの外部エンジン接続に関する情報を表示します。

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                              Server-       Server-
Vserver          Policy    Node          Server        status        type
---------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1   node1        10.1.1.2      connected     primary
vs1.example.com policy1   node1        10.1.1.3      disconnected  primary
vs1.example.com policy1   node2        10.1.1.2      connected     primary
vs1.example.com policy1   node2        10.1.1.3      disconnected  primary
```

この例は、接続されているFPolicyサーバに関する情報のみを表示します。

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver          policy-name server
---------- ---------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2
```

FPolicyパススルーリード接続のステータスに関する情報を表示する

クラスタまたは指定したStorage Virtual Machine（SVM）の外部FPolicyサーバ（FPolicyサーバ）へのFPolicyパススルーリード接続のステータスに関する情報を表示できます。この情報は、パススルーリードデータ接続が確立されているFPolicyサーバや、パススルーリード接続が切断されているFPolicyサーバを確認するのに役立ちます。

タスクの内容

いずれのパラメータも指定しない場合、次の情報が表示されます。

- SVM名
- FPolicyポリシー名
- ノード名
- FPolicyサーバのIPアドレス
- FPolicyパススルーリード接続のステータス

クラスタまたは特定のSVMのFPolicy接続に関する情報の表示に加え、コマンドパラメータを使用して、他の条件によってコマンドの出力をフィルタリングすることができます。

パラメータを指定すると、リストされているポリシーに関する詳細情報を表示できます `-instance`。また、パラメータを使用して、指定したフィールドのみをコマンド出力に表示することもできます `-fields`。パラメータのあとに `-fields`と入力すると、使用できるフィールドを確認できます `?`。

ステップ

1. 適切なコマンドを使用して、ノードとFPolicyサーバの間の接続ステータスに関する情報をフィルタリングして表示します。

表示する接続ステータス情報	入力するコマンド
クラスタのFPolicyパススルーリード接続ステータス	`vserver fpolicy show-passthrough-read-connection`
指定したSVMのFPolicyパススルーリード接続ステータス	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`
指定したポリシーのFPolicyパススルーリード接続ステータス	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
指定したポリシーの詳細なFPolicyパススルーリード接続ステータス	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`
指定したステータスのFPolicyパススルーリード接続ステータス	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status`サーバのステータスは、次のいずれかになります。 • `connected` • `disconnected`

例

次のコマンドは、クラスタ上のすべてのFPolicyサーバからのパススルーリード接続に関する情報を表示します。

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                          FPolicy           Server
Vserver          Policy Name   Node       Server            Status
---------------  ------------- ---------- ----------------- --------------
vs2.example.com  pol_cifs_2    FPolicy-01   2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
```

次のコマンドは、「 pol_cifs_1 」ポリシーに設定されている FPolicy サーバからのパススルーリード接続に関する詳細情報を表示します。

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                          Node: FPolicy-01
                                       Vserver: vs1.example.com
                                        Policy: pol_cifs_1
                                        Server: 1.1.1.1
               Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                  Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

著作権に関する情報

商標に関する情報