FPolicyとは

ONTAP 9

NetApp
January 23, 2026

目次

FPolicyとは

ONTAP FPolicyソリューションについて学ぶ

FPolicyは、パートナー ソリューション経由でStorage Virtual Machine（SVM）上のファイル アクセス イベントを監視、管理するため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に役立ちます。

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Workload SecurityおよびCloud Data Senseが含まれます。

FPolicyソリューションは2つの部分で構成されます。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。ONTAP FPolicyが送信した通知は、お客様のユースケースを満たすために、外部FPolicyサーバによって処理されます。

ONTAPフレームワークは、FPolicy設定の作成と維持、ファイルイベントの監視、外部FPolicyサーバへの通知の送信を行います。ONTAP FPolicyは、外部FPolicyサーバとストレージ仮想マシン（SVM）ノード間の通信を可能にするインフラストラクチャを提供します。

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 イベントが発生すると、FPolicyサーバに通知を送信します。外部FPolicyサーバは通知を処理し、ストレージ ノードに応答を返します。通知処理の結果は、アプリケーション、およびストレージ ノードと外部サーバ間の通信が非同期か同期かによって異なります。

ONTAP FPolicyの同期および非同期通知

FPolicyでは、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。通知の送信方法には同期モードと非同期モードの2種類があり、通知モードによって、FPolicyサーバへの通知送信後の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処理を続行するため、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、その評価結果に基づいてFPolicyサーバで処理を行う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。

  非同期モードで動作しているFPolicyサーバでネットワーク障害が発生した場合、障害発生中に生成されたFPolicy通知はストレージ ノードに保存されます。FPolicyサーバがオンラインに復帰すると、保存された通知が通知され、ストレージ ノードから取得できます。障害発生中に通知を保存できる時間は、最大10分まで設定可能です。

  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。

- 同期通知

  同期モードで実行するように設定した場合は、すべての通知についてFPolicyサーバからの確認応答を受け取るまで、クライアントは処理を続行できません。このタイプの通知は、その評価結果に基づいて処理を行う必要がある場合に適しています。たとえば、SVM管理者が要求を許可するかどうかを外部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します。

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さまざまな用途があり、非同期と同期の両方に対応しています。

非同期アプリケーションとは、外部FPolicyサーバがファイルやディレクトリへのアクセスを変更したり、Storage Virtual Machine（SVM）上のデータを変更したりし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 リソースの管理

同期アプリケーションとは、外部FPolicyサーバによってデータアクセスが変更されたり、データが修正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

ONTAP FPolicy 永続ストア

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、FPolicy 永続ストアの設定が簡素化されました。 `persistent-store create`コマンドは、SVM のボリューム作成を自動化し、永続ストアのベスト プラクティスに基づいてボリュームを設定します。

永続ストアのベスト プラクティスの詳細については、"FPolicy を構成するための要件、考慮事項、およびベストプラクティス"を参照してください。

永続ストアの追加については、"永続的ストアの作成"を参照してください。

ONTAP 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、通知を受けて処理と対応を行う外部FPolicyサーバを使用します。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**サーバー設定

  FPolicyサーバに通知が送信され、そのサーバが要求をスクリーニングし、要求されたファイル処理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処理を許可または拒否する応答をノードに送信します。

- ネイティブ **FPolicy** サーバ設定

  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。

  注意：拒否されたファイル拡張子の要求は記録されません。

ネイティブ**FPolicy**設定を作成するタイミング

ネイティブFPolicy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だけで十分な場合、ネイティブファイルブロッキング設定の使用が適切です。

ネイティブ ファイル ブロッキングを使用すると、設定し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処理を監視したうえで、特定の拡張子のファイルへのアクセスを拒否することができます。これはデフォルトの設定です。

この設定により、ファイルの拡張子のみに基づいてファイルアクセスをブロックできます。例えば、 `mp3`拡張子を含むファイルをブロックするには、対象のファイル拡張子が `mp3`である特定の操作に対して通知を送信するポリシーを設定します。このポリシーは、通知を生成する操作に対する `mp3`ファイルリクエストを拒否するように設定されています。

ネイティブFPolicy設定には次の条件が適用されます。

- FPolicyサーバベース 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サーバベースのファイル 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、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 ブロッキング機能では、ファイルの内容でなく、拡張子のみに基づいてファイルがスクリーニングされます。
- シンボリック リンクの場合には、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。

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

外部FPolicyサーバを使用する設定を作成する状況

ファイル拡張子に基づいて単にファイルをブロックする以上のことが求められるユース ケースの場合、通知の処理と管理に外部FPolicyサーバを使用するようにFPolicyを設定することは、堅牢なソリューションとなります。

ファイル アクセス イベントの監視および記録、クォータ サービスの提供、単純なファイルの拡張子以外の基準に基づくファイル ブロッキング、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、Storage Virtual Machine（SVM）内のデータのサブセットのみを監視する詳細なポリシー セットの提供などの状況では、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。

ONTAP FPolicy実装におけるクラスタコンポーネントの役割

FPolicyの実装においては、クラスタ、クラスタに含まれるStorage Virtual Machine（SVM）、およびデータLIFのそれぞれに役割があります。

- 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、クラスタ内のすべてのFPolicy設定に関する情報をクラスタが管理します。

- **SVM**

  FPolicy設定はSVMレベルで定義されます。設定対象はSVMであり、SVMリソースにのみ適用されます。あるSVM設定で、別のSVMにあるデータへのファイル アクセス要求を監視し、通知を送信することはできません。

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

- **data LIF**

  FPolicyサーバへの接続は、FPolicy設定の対象である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。

ONTAP 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が実行されるようになります。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サーバとやり取りする通知メッセージの管理を行います。

さらに、接続管理の一環として、FPolicy には次の責任があります：

- ファイル通知が正しいLIFを通過してFPolicyサーバに送信されるようにする。

- 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行われるようにする。
- FPolicyサーバへの接続が切断されたときに再接続を試行する。
- 認証されたセッションを介してFPolicyサーバに通知を送信する。
- パススルー リードが有効な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 データ接続を管理する。

制御チャネルを使用した**FPolicy**通信

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。

権限付きデータ アクセス チャネルを使用した同期通信

同期通信では、FPolicyサーバは、特権データ 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。特権パスを介したアクセスでは、FPolicyサーバにファイルシステム全体が公開されます。サーバは、データ ファイルにアクセスして情報を収集したり、ファイルのスキャン、ファイルの読み取り、またはファイルへの書き込みを行ったりできます。

外部FPolicyサーバが特権データ 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、特権データ チャネル接続はセキュアである必要があります。

FPolicy接続認証情報が特権データアクセスチャネルで使用される仕組み

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特権データ アクセス接続を確立します。特権データ アクセス チャネル接続の確立用としてサポートされているプロトコルは、SMBだけです。

FPolicyサーバで特権データ アクセスが必要となる場合は、次の条件を満たす必要があります。

- クラスタでSMBライセンスが有効になっている。
- FPolicy サーバーは、FPolicy 設定で設定された資格情報に基づいて実行する必要があります。

データ チャネル接続を確立するとき、FPolicyでは、指定されたWindowsユーザ名のクレデンシャルが使用されます。データ アクセスは、管理共有ONTAP_ADMIN$を介して確立されます。

権限付きデータ アクセスのためのスーパー ユーザ クレデンシャルの付与とは

ONTAPは、IPアドレスとFPolicyに設定されたユーザ 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際に次の権限を付与します。

- 権限チェックの省略

  ファイルやディレクトリに対するアクセスのチェックが省略されます。

- 特別なロック権限

ファイルにロックが設定されていても、読み取り、書き込み、変更が許可されます。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、そのファイルの既存のロックはその時点で解除されます。

- すべてのFPolicyチェックのバイパス

  アクセス時にFPolicy通知が生成されません。

FPolicyによるポリシー処理の管理方法

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設定を作成するには、FPolicyがどのようにポリシー処理を管理するかを理解しておくことが重要です。

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

ポリシーの設定時には、次の推奨事項を考慮してください。

- あるポリシーが常に他のポリシーより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。
- 監視対象イベントに対して要求されたファイル アクセス処理の成功が、別のポリシーで評価されるファイル要求の前提条件になっている場合は、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設定します。

  たとえば、あるポリシーがFPolicyのファイル アーカイブとリストアを管理し、2つ目のポリシーがオンライン ファイルへのファイル アクセス処理を管理する場合は、ファイル リストアを管理するポリシーの優先度を高く設定し、2つ目のポリシーが管理する処理が許可される前にファイルがリストアされるように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があるすべてのポリシーを評価するには、同期ポリシーの優先度を低く設定します。

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、新しい優先度に基づいてFPolicyでポリシーを評価するには、シーケンス番号を変更した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。

ノードと外部のONTAP FPolicyサーバ間の通信プロセス

FPolicy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。

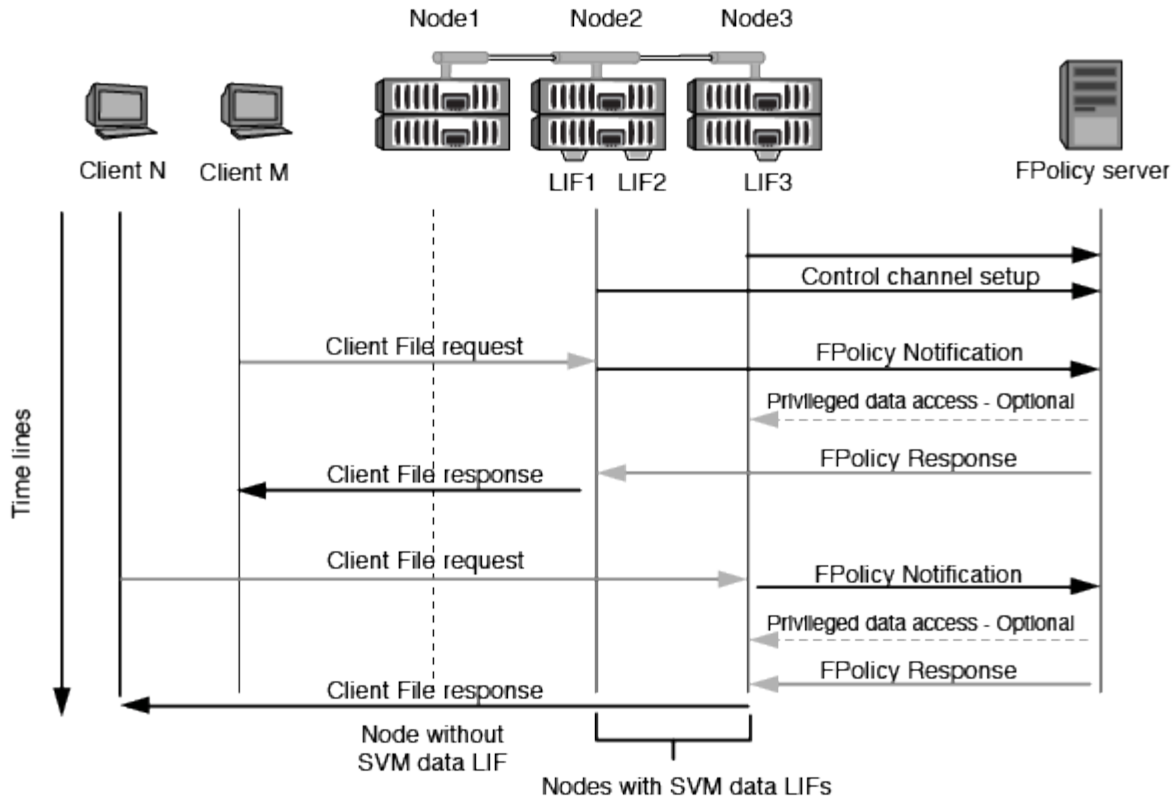
Storage Virtual Machine（SVM）に属しているすべてのノードは、TCP/IPを使用して外部FPolicyサーバへの接続を開始します。FPolicyサーバへの接続のセットアップには、ノードのデータLIFを使用します。そのため、接続のセットアップは、ノードでSVMのデータLIFが稼働している場合しか実行できません。

ポリシーが有効になっている場合は、各ノードのそれぞれのFPolicyプロセスで、FPolicyサーバとの接続の確立が試行されます。これには、ポリシーの設定で指定された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のアドレスとして同じノードでIPv4とIPv6の両方が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。そのため、SVMが複数のノードに展開されている場合、またはIPv4とIPv6の両方のアドレス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にLIF2からの制御チャネルの確立を試みます。



LIFの移行またはフェイルオーバー時における**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きは、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と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における**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 ノードに障害が発生した場合は、FPolicyサーバとノードの間の接続が切断されます。

クラスタ フェイルオーバーがFPolicyサーバに与える影響は、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。移行が完了したら、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。ノードが稼働したら、新しいセッションIDを使用してそのノードから新しい接続が開始されます。

FPolicyサーバでは、切断された接続を検出するためにキープアライブ プロトコル メッセージが使用されます。セッションIDをパージするためのタイムアウトは、FPolicy設定時に決定します。デフォルトのキープアライブのタイムアウトは2分です。

SVM ネームスペース全体にわたる ONTAP FPolicy サービスについて学ぶ

ONTAPは、統合ストレージ仮想マシン（SVM）ネームスペースを提供します。クラスタ全体のボリュームはジャンクションによって結合され、単一の論理ファイルシステムを提供します。FPolicyサーバーはネームスペースのトポロジを認識し、ネームスペース全体にFPolicyサービスを提供します。

名前空間はSVMに固有のものであり、SVM内に含まれるため、SVMのコンテキストからのみ参照できます。名前空間には以下の特性があります：

- 各SVMには1つのネームスペースが存在し、ネームスペースのルートはルートボリュームであり、ネームスペースではスラッシュ（/）として表されます。
- 他のすべてのボリュームには、ルート（/）の下にジャンクション 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 エクスポートで完全な名前空間へのアクセスを提供できます。それ以外の場合は、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。
- SMB 共有は、ボリューム上、ボリューム内の qtree 上、または名前空間内の任意のディレクトリ上に作成できます。
- 名前空間のアーキテクチャは柔軟です。

  一般的な名前空間アーキテクチャの例は次のとおりです：

  - ルートから単一のブランチを持つ名前空間
  - ルートから複数のブランチを持つ名前空間
  - ルートから分岐していない複数のボリュームを持つネームスペース

ONTAP FPolicyパススルーリードが階層型ストレージ管理の使いやすさを向上させる仕組み

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（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。

FPolicyサーバがSMBサーバ上にあるファイルに対してHSMを提供するように構成されている場合は、ポリシ

ーベースのファイル移行が行われます。この場合、ファイルはセカンダリ ストレージ上にオフライン格納され、スタブ ファイルのみがプライマリ ストレージ上に残ります。たとえクライアントからは通常のファイルのように見えても、スタブ ファイルは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 ファイルは、SMBのオフライン 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。

通常は、オフライン ファイルに対する読み取り要求が届くと、プライマリ ストレージ上への要求されたコンテンツのリコール（呼び戻し）を行ったうえで、プライマリ ストレージを介してそのコンテンツに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ことから、いくつかの好ましくない影響が生じます。特に、コンテンツをリコールしてから要求に応じる必要があるためにクライアント要求に対する遅延が大きくなる点と、プライマリ ストレージで必要となる領域の使用量がリコールされるファイルのサイズだけ増える点が挙げられます。

FPolicyのパススルー 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）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。プライマリ ストレージにファイルをリコールして戻す代わりに、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 リードは、次のような利点を提供してユーザビリティを向上します。

- 要求されたデータをリコールするための十分な領域がプライマリ ストレージになくても、読み取り要求を処理できます。
- スクリプトまたはバックアップ ソリューションで多数のオフライン ファイルへのアクセスが必要になる場合など、データのリコールが急増した場合でも容量やパフォーマンスの管理を適切に行うことができます。
- スナップショット内のオフライン ファイルの読み取り要求を処理できます。

  スナップショットは読み取り専用であるため、スタブファイルがスナップショット内に存在する場合、FPolicyサーバーは元のファイルを復元できません。パススルー読み取りを使用すると、この問題は解消されます。

- セカンダリ ストレージ上のファイルへのアクセスによって読み取り要求が処理されるタイミングや、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 ファイルをプライマリ ストレージ上に移行し直すまでの指定され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）および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け取ると、FPolicyによって標準の接続チャネル経由でFPolicyサーバ（HSMサーバ）に通知が送信されます。

通知を受け取ったあと、FPolicyサーバはその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およびFPolicy間に確立されたパススルー リード特権データ接続を介してSVMに送信します。

このデータの送信後、FPolicyサーバは読み取り要求にALLOW（許可）またはDENY（拒否）で応答します。読み取り要求が許可されたか拒否されたかによって、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。

著作権に関する情報

商標に関する情報