FPolicyについて

ONTAP 9

NetApp
April 24, 2024

目次

FPolicyについて

FPolicy 解決策の 2 つの要素とは何ですか

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 解決策は 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。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 フレームワークでは、外部 FPolicy サーバへの接続を確立し、クライアントアクセスによっ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、そ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、アプリケーションごとに異なるほか、ノードと外部サーバの間の通信が非同期と同期のどちらであるかによっても異なります。

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、 FPolicy サーバからの応答を待たずにノードでの処理を継続できるため、システムの全体的なスループットが向上します。この種類の通知は、通知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されます。

  非同期モードで動作している FPolicy サーバでネットワーク停止が発生した場合、停止中に生成された FPolicy 通知は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、サーバは格納された通知に関するアラートを受け取り、ストレージノードから通知を読み込むことができます。停止中に通知を保存できる期間は、最大 10 分に設定できます。

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

- * 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ってからでないと、クライアントの処理を続行できません。このタイプの通知は、通知の評価結果に基づいて処理を行う必要がある場合に使用されます。たとえば、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、ファイルまたは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、データアクセスやデータが外部 FPolicy サーバによって変更されるアプリケーションです。例：

- クォータ管理
- ファイルアクセスブロッキング
- ファイル・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

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

この機能は、FPolicy外部モードでのみ使用できます。この機能をサポートするには、使用するパートナーアプリケーションが必要です。このFPolicy設定がサポートされていることをパートナーと協力して確認する必要があります。

ベストプラクティス

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設定する必要があります。永続ストアが設定されている場合、一致するすべてのFPolicyイベントがキャプチャされ、FPolicyパイプライン内でさらに処理されて外部サーバに送信されます。

永続ストアは、予期しないリブートが発生した場合、またはFPolicyを無効にして再度有効にした場合に、最後のイベントを受信した時点のままになります。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。再実行する必要があります `fpolicy persistent-store create` ボリュームの移動後にいずれかのノードでコマンドを実行し、保留中の通知が外部サーバに配信されるようにします。

永続的ストアボリュームはSVM単位でセットアップします。FPolicyが有効なSVMごとに、永続的ストアボリュームを作成する必要があります。

FPolicyで最大トラフィック量を監視すると想定されるLIFがあるノードに永続的ストアボリュームを作成します。

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は該当するEMSメッセージを含む受信通知を破棄し始めます。

永続的なストアのボリューム名とボリューム作成時に指定したジャンクションパスが一致している必要があります。

Snapshotポリシーをに設定 `none` 対象のボリュームではなく `default`。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。

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。これには、FPolicyを有効にしたあとに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すると、ユーザプロトコルアクセスができなくなります。

詳細については、を参照してください "永続ストアの作成"。

FPolicy の設定タイプ

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 サーバ構成 *

  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。

を使用してネイティブ **FPolicy** 設定を作成する場合

ネイティブの FPolicy 設定では、 ONTAP に組み込まれている 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。この解決策には、外部 FPolicy サーバ（ FPolicy サーバ）は必要ありません。ネイティブファイルブロッキングの設定は、このシンプルな解決策がすべて必要な場合に適しています。

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、特定の拡張子を持つファイルへのアクセスを拒否することができます。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、を含むファイルをブロックします `mp3` 拡張子を使用すると、ターゲットのファイル拡張子がの特定の処理に関する通知を送信するようにポリシーを設定できます `mp3`。ポリシーは拒否するように設定されています `mp3` 通知を生成する操作に対するファイル要求。

次の環境ネイティブ FPolicy の設定：

- 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のために設定したポリシーで、もう 1 つは FPolicy のサーバベースのファイルスクリーニングのために設定したポリシーです。

- ネイティブファイルブロッキング機能では、ファイルの内容ではなく、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、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。

の詳細を確認してください "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が必要なユースケースに対して、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、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など、目的に応じて外部 FPolicy サーバを使用する設定を作成する必要があります。 または、 Storage Virtual Machine （ SVM ）の一部のデータのみを監視するきめ細かいポリシーセットを提供することもできます。

FPolicy 実装でクラスタコンポーネントが果たす役割

FPolicy の実装においては、クラスタ、それに含まれる 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 *

クラスタに含まれる FPolicy の管理フレームワークで、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 であり、 SVM リソースにのみ適用されます。1 つの SVM 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 を通じて行われます。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。

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場合、再接続を試行します。
- 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。

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、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。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 の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 サーバで権限付きデータアクセスが必要とされる場合は、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必要があります。
- FPolicy サーバが FPolicy の設定で指定されたクレデンシャルで実行されている。

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何ですか

ONTAP は、 IP アドレスと FPolicy 設定で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。

スーパーユーザには、 FPolicy サーバでデータにアクセスする際に次の権限が付与されます。

- 権限チェックの省略

  ファイルやディレクトリへのアクセスのチェックが省略されます。

- 特殊なロック権限

  ONTAP では、ロックが設定されていても、ファイルへの読み取り、書き込み、変更が許可されます。バイト単位のロックが設定されたファイルを FPolicy サーバで取得した場合、ファイルに対する既存のロックはすぐに解除されます。

- すべての FPolicy チェックを省略します

  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。

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するポリシーが決定されます。監視対象イベントの場合は、関連するポリシーとともにそのイベントに関する情報が評価を行う 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してください。

- ある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正常に実行されることが、別のポリシーに対して評価されるファイル要求の前提条件となる場合は、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、 1 つのポリシーで FPolicy のファイルのアーカイブとリストアの機能を管理し、 2 つ目のポリシーでオンラインファイルのファイルアクセス処理を管理する場合、 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、 2 番目のポリシーで管理されている処理を実行する前にファイルをリストアす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、変更した優先度に基づいてポリシーを評価するには、変更したシーケンス番号を持つ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

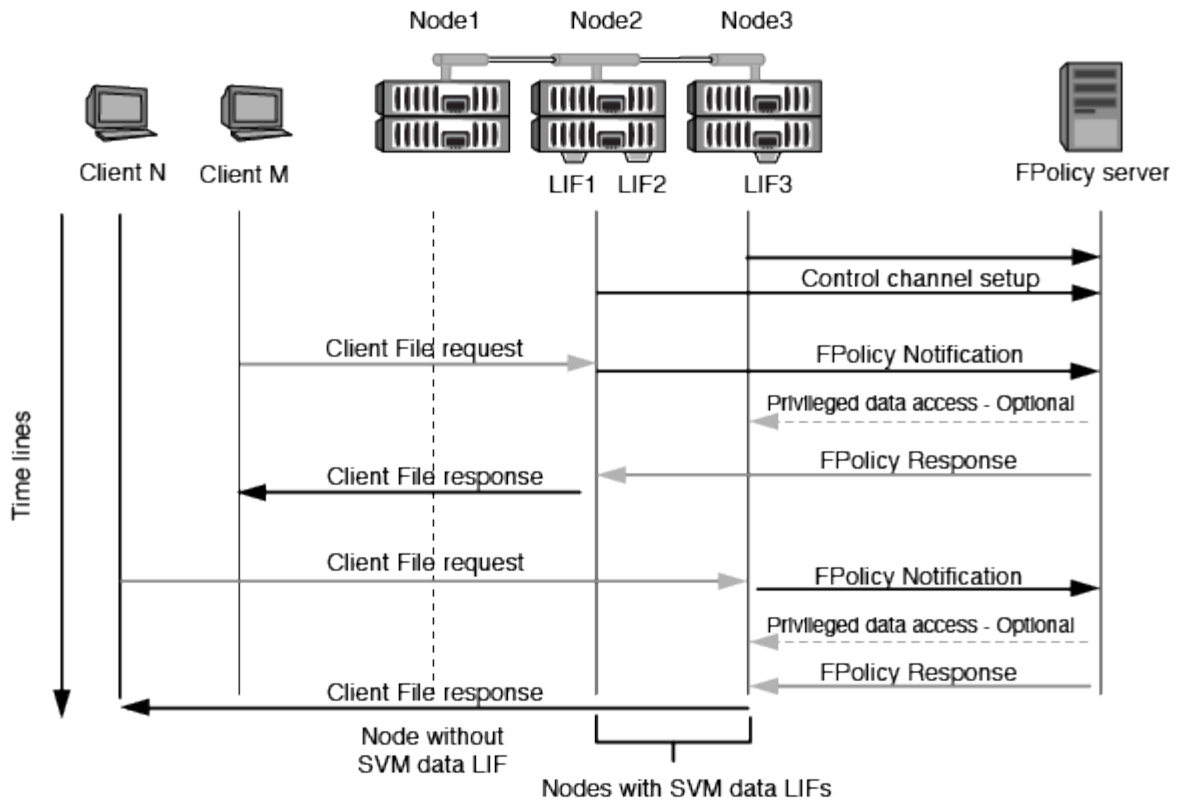
FPolicy の設定を適切に計画するには、ノードと外部 FPolicy サーバの間の通信プロセスについて理解しておく必要があります。

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。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。また、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、クラスタのノードが 3 つ（ノード 1 、ノード 2 、ノード 3 ）ある場合に、 SVM のデータ LIF がノード 2 とノード 3 にのみ分散されていると、データボリュームの分散に関係なく、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 には LIF1 と LIF2 の 2 つのデータ LIF があり、これらは SVM に属しており、初期接続は LIF1 からであるとします。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、 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、 ONTAP 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 の設定時に決定します。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 のパススルーリードによる階層型ストレージ管理の利便性向上

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。

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、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から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レイテンシが大きくなる点と、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スペース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。
- スクリプトやバックアップ解決策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。
- 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がプライマリストレージに移行されるまでの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 ）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。