



FPolicy イベントの設定を計画する

ONTAP 9

NetApp
December 20, 2024

目次

FPolicyイベントの設定を計画する	1
FPolicyイベントの設定の概要を計画する	1
FPolicyでSMBヲカンシスルタメニサポートサレルファイルソウサトフィルタノクミアワセ	5
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)	6
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)	8
FPolicyイベント設定ワークシートに記入する	10

FPolicyイベントの設定を計画する

FPolicyイベントの設定の概要を計画する

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

FPolicyイベントを作成することの意味

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

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

FPolicyは、SMB、NFSv3、NFSv4のファイルアクセス処理を監視できます。ONTAP 9.15.1以降では、NFSv4.1のファイルアクセス処理も監視できます。

- 監視するファイル処理

すべてのファイル処理が、各プロトコルに対して有効とは限りません。

- 構成するファイル フィルタ

ファイル処理とフィルタの特定の組み合わせだけが有効です。プロトコルごとに、サポートされる独自の組み合わせがあります。

- ボリュームのマウントおよびアンマウント操作を監視するかどうか

3つのパラメータ(-protocol、-file-operations、-filters) との依存関係があります。3つのパラメータの有効な組み合わせは次のとおりです。





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

FPolicyイベントの設定内容

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

情報の種類	オプション
-------	-------

<p>SVM</p> <p>このFPolicyイベントに関連付けるSVMの名前を指定します。</p> <p>各FPolicy設定は、単一のSVM内で定義されます。FPolicyポリシーの構成要素となる外部エンジン、ポリシーイベント、ポリシーのスコープ、およびポリシーを、すべて同じSVMに関連付ける必要があります。</p>	<p>-vserver vserver_name</p>
<p>_ イベント名 _</p> <p>FPolicyイベントに割り当てる名前を指定します。FPolicyポリシーを作成するときは、イベント名を使用してFPolicyイベントをポリシーに関連付けます。</p> <p>名前の最大文字数は256文字です。</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> MetroClusterまたはSVMディザスタリカバリ設定でイベントを設定する場合、この名前は最大200文字にする必要があります。</p> </div> <p>名前には、次のASCII文字の任意の組み合わせを含めることができます。</p> <ul style="list-style-type: none"> • a`から `z • A`から `Z • 0`から `9 • _ `"'、"'、"'。"'-`", and " 	<p>-event-name event_name</p>
<p>プロトコル _</p> <p>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。</p> <ul style="list-style-type: none"> • cifs • nfsv3 • nfsv4 <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> 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。</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> 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。</p> </div>	<p>-protocol protocol</p>

_ ファイル操作 _

FPolicyイベントのファイル操作のリストを指定します。

このイベントは、パラメータで指定したプロトコルを使用して、すべてのクライアント要求からこのリストに指定された操作をチェックします `-protocol`。1つ以上のファイル操作をカンマで区切って指定できます。のリスト `-file-operations` には、次の値を1つ以上指定できます。

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



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

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

_ フィルタ _

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。

<p>は、ボリューム処理が必要です _</p> <p>ボリュームのマウントおよびアンマウント操作に対して監視が必要かどうかを指定します。デフォルトは false。</p>	<pre>-volume-operation{true</pre>
<pre>false}</pre> <p>-filters `filter`はい。</p>	<p><i>FPolicy</i>アクセスが通知を拒否しました</p> <p>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。</p> <ul style="list-style-type: none"> • Failures due to NTFS permissions. • Failures due to Unix mode bits. • Failures due to NFSv4 ACLs.
<pre>-monitor-fileop-failure{true</pre>	<pre>false}</pre>

FPolicyでSMBのファイルアクセスイベントを監視する際のサポートされるファイル操作とフィルタの組み合わせ

`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		

著作権に関する情報

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

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

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

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

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

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

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

商標に関する情報

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