



FPolicy設定の作成

ONTAP 9

NetApp
February 12, 2026

目次

FPolicy設定の作成	1
ONTAP FPolicy外部エンジンを作成する	1
ONTAP FPolicyイベントを作成する	2
FPolicyイベントの作成	2
FPolicyアクセス拒否イベントの作成	3
ONTAP FPolicy永続ストアを作成する	3
永続的ストアの作成（ONTAP 9.15.1以降）	3
永続的ストアの作成（ONTAP 9.14.1）	4
ONTAP FPolicyポリシーを作成する	5
ONTAP FPolicyスコープを作成する	7
ONTAP FPolicyポリシーを有効にする	8

FPolicy設定の作成

ONTAP FPolicy外部エンジンを作成する

FPolicy設定を作成するには、最初に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で外部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がないので、この手順の実行は不要です。

開始する前に

"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。

タスク概要

外部エンジンがMetroCluster構成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 サイトでのFPolicyサーバのIPアドレスは、セカンダリ サーバとして指定してください。

手順

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

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一切必要ありません。

```
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. `vserver fpolicy policy external-engine show` 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。

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 Type	Engine	Servers	Servers	Port	Engine
-----	-----	-----	-----	-----	
vs1.example.com synchronous	engine1	10.1.1.2, 10.1.1.3	-	6789	

次のコマンドは、SVM vs1.example.com 上の「engine1」という名前の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: -
```

ONTAP FPolicyイベントを作成する

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ポリシーを作成するときに、このイベントをポリシーに関連付けます。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["ワークシート"](#)を完了する必要があります。

FPolicyイベントの作成

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

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

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

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

FPolicyアクセス拒否イベントの作成

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

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

ONTAP FPolicy永続ストアを作成する

永続ストアは、クライアントのI/O処理とFPolicy通知処理を分離することで、クライアントのレイテンシを削減するのに役立ちます。ONTAP 9.14.1以降では、FPolicyを使用して"**永続ストア**"を設定し、SVM内の非同期の非必須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（必須または非必須）および非同期の必須設定はサポートされていません。

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、永続ストア用のボリュームを設定します。

永続的ストアの作成方法は、ONTAPリリースによって2種類に分かれます。

- ONTAP 9.15.1 以降：永続ストアを作成すると、ONTAP は同時にボリュームの作成と設定を自動的行います。これにより、FPolicy 永続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および設定し、新しく作成したボリュームの永続ストアを作成します。

SVMごとに設定できる永続的ストアは1つだけです。ポリシーの提供パートナーが異なる場合でも、各SVM上のすべてのFPolicy設定に単一の永続的ストアを使用する必要があります。

永続的ストアの作成（ONTAP 9.15.1以降）

ONTAP 9.15.1以降では、`fpolicy persistent-store create` コマンドを使用して、インラインボリュームの作成と設定を含むFPolicy永続ストアを作成できます。ONTAPは、ボリュームへの外部ユーザープロトコル アクセス（CIFS/NFS）を自動的にブロックします。

開始する前に

- 永続的ストアの作成先となるSVMには、アグリゲートを1つ以上用意しておく必要があります。
- SVM用アグリゲートへのアクセス権と、ボリューム作成の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。この際、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、`volume show` コマンドを使用してそのボリュームを検索し、ボリューム パラメータで指定します。

- `size` パラメータは、外部サーバー（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30,000件の通知があるクラスターで、イベントを30分間維持する場合のサイズは、次のように計算します。

必要なボリューム サイズ = $30000 \times 30 \times 60 \times 0.6\text{KB}$ （平均通知レコード サイズ） = 32400000 KB = 約32 GB

おおよその通知レートを確認するには、FPolicy パートナー アプリケーションにアクセスするか、FPolicy カウンター `requests_dispatched_rate` を使用します。



既存のボリュームを使用する場合、size パラメータは省略可能です。size パラメータの値を指定すると、ボリュームのサイズが指定したものに變更されます。

- `autosize-mode` パラメータは、ボリュームの自動サイズ調整モードを指定します。サポートされている自動サイズ調整モードは次のとおりです：
 - off - スペースの使用状況が変化しても、サイズの拡張も縮小も行いません。
 - grow - ボリュームのスペースの使用量が拡張しきい値を超えた場合に、ボリュームを自動的に拡張します。
 - grow_shrink - スペース使用量の増減に合わせてボリュームを拡張または縮小します。

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、["FPolicy ポリシーの作成"](#)を参照してください。

永続的ストアの作成（ONTAP 9.14.1）

ボリュームを作成してから、そのボリュームを使用する永続的ストアを作成します。その後、新しく作成したボリュームに対する外部ユーザのプロトコル アクセス（CIFS および NFS）をブロックできます。

手順

1. 永続ストア用にプロビジョニングできる空のボリュームを 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 権限（ボリュームを作成するための）を持つ管理者ユーザーが、必要なサイズのボリューム（`volume cli` コマンドまたは REST API を使用）を作成し、そのボリュームの名前を persistent store create CLI コマンドまたは REST API の `volume` として指定することが想定されています。

- `vserver` パラメータは SVM の名前です。

- `volume` パラメーターは永続ストア ボリュームの名前です。
- `state` パラメータは、ボリュームを使用できるようにするためにオンラインに設定する必要があります。
- `policy` パラメータは、既に設定されている場合、FPolicy サービスポリシーに設定されます。設定されていない場合は、後で `volume modify` コマンドを使用してポリシーを追加できます。
- `unix-permissions` パラメータはオプションです。
- `size` パラメーターは、外部サーバー（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30,000件の通知があるクラスターで、イベントを30分間維持する場合のサイズは、次のように計算します。

必要なボリューム サイズ = 30000 x 30 x 60 x 0.6KB（平均通知レコード サイズ） = 32400000 KB = 約32 GB

おおよその通知レートを確認するには、FPolicy パートナー アプリケーションにアクセスするか、FPolicy カウンター `requests_dispatched_rate` を使用します。

- `aggregate` パラメータは、FlexVol ボリュームを使用する場合は必須です。それ以外の場合は省略可能です。
- `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復元されて現在のイベントが失われることがなくなり、イベント処理が重複する可能性も回避されます。

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

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` パラメーターは永続ストア 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、["FPolicy ポリシーの作成"](#)を参照してください。

ONTAP FPolicy ポリシーを作成する

FPolicy ポリシーを作成する際には、外部エンジンと1つ以上のイベントをこのポリシーに関連付けます。このポリシーでは、必須のスクリーニングが要求されるかどうか、FPolicy サーバに Storage Virtual Machine (SVM) 上のデータへの特権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も指定します。

開始する前に

- 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つは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構成するには、エンジン タイプが **async** であり、ポリシーが **non-mandatory** である必要があります。

詳細については、"[永続的ストアの作成](#)"を参照してください。

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 1 つ以上のイベントを追加できます。
- デフォルトでは、必須スクリーニングが有効になっています。
- `-allow-privileged-access` パラメータを `yes` に設定して特権アクセスを許可する場合は、特権アクセス用の特権ユーザー名も設定する必要があります。
- `-is-passthrough-read-enabled` パラメータを `true` に設定してパススルー読み取りを構成する場合は、特権データ アクセスも構成する必要があります。

次のコマンドは、「policy1」という名前のポリシーを作成します。このポリシーには、「event1」という名前のイベントと「engine1」という名前の外部エンジンが関連付けられています。このポリシーでは、ポリシー設定で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、「policy2」という名前のポリシーを作成します。このポリシーには、「event2」という名前のイベントと「engine2」という名前の外部エンジンが関連付けられています。このポリシーは、指定されたユーザー名を使用して特権アクセスを使用するように構成されています。パススルー読み取りが有効になっています：

```
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」というポリシーを作成します。このポリシーはネイティブ エンジンを使用し、ポリシー設定のデフォルト値を使用します：

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


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

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た SVM
- ポリシーに関連付けられた外部エンジン
- ポリシーに関連するイベント
- 強制検査が必要かどうか
- 特権アクセスが必要かどうか `vserver fpolicy policy show`

Vserver	Policy Name	Events	Engine	Is Mandatory	Privileged 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

ONTAP 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際は、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境界を定義します。スコープでは、共有、エクスポート ポリシー、ボリューム、ファイル拡張子に基づいて、ファイルを含めるか除外するかを指定できます。

開始する前に

FPolicy スコープワークシートに記入してください。FPolicy ポリシーは、関連付けられた外部エンジン（ポリシーが外部 FPolicy サーバを使用するように設定されている場合）と共に存在し、少なくとも1つの関連付けられた FPolicy イベントを持っている必要があります。

手順

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

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

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

```
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: -
```

ONTAP 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、ポリシーの優先度が設定され、ポリシーのファイルアクセス監視が開始されます。

開始する前に

FPolicyポリシーは、関連付けられた外部エンジン（ポリシーが外部FPolicyサーバを使用するように設定されている場合）と共に存在し、少なくとも1つの関連付けられたFPolicyイベントを持っている必要があります。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。

タスク概要

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。標準的なエンジンの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、その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 でポリシーを有効にできません。

手順

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

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

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

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

著作権に関する情報

Copyright © 2026 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。