



Creare la configurazione FPolicy

ONTAP 9

NetApp
February 12, 2026

Sommario

Creare la configurazione FPolicy	1
Creare motori esterni ONTAP FPolicy	1
Crea eventi ONTAP FPolicy	2
Creare l'evento FPolicy	2
Creare gli eventi di accesso negato FPolicy	3
Crea archivi persistenti ONTAP FPolicy	3
Creare un archivio permanente (ONTAP 9.15.1 o versione successiva)	3
Creare un archivio persistente (ONTAP 9.14.1)	4
Creare policy ONTAP FPolicy	5
Crea ambiti ONTAP FPolicy	7
Abilitare le policy ONTAP FPolicy	8

Creare la configurazione FPolicy

Creare motori esterni ONTAP FPolicy

È necessario creare un motore esterno per iniziare a creare una configurazione FPolicy. Il motore esterno definisce il modo in cui FPolicy crea e gestisce le connessioni ai server FPolicy esterni. Se la configurazione utilizza il motore ONTAP interno (il motore esterno nativo) per un semplice blocco dei file, non è necessario configurare un motore esterno FPolicy separato e non è necessario eseguire questa operazione.

Prima di iniziare

Il ["motore esterno"](#) il foglio di lavoro deve essere completato.

A proposito di questa attività

Se il motore esterno viene utilizzato in una configurazione MetroCluster, è necessario specificare gli indirizzi IP dei server FPolicy nel sito di origine come server primari. Gli indirizzi IP dei server FPolicy nel sito di destinazione devono essere specificati come server secondari.

Fasi

1. Creare il motore esterno FPolicy utilizzando `vserver fpolicy policy external-engine create` comando.

Il seguente comando crea un motore esterno su una macchina virtuale di storage (SVM) `vs1.example.com`. Non è richiesta alcuna autenticazione per le comunicazioni esterne con il server FPolicy.

```
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. Verificare la configurazione del motore esterno FPolicy utilizzando `vserver fpolicy policy external-engine show` comando.

Il seguente comando visualizza le informazioni su tutti i motori esterni configurati su SVM `vs1.example.com`:

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

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

Il seguente comando visualizza informazioni dettagliate sul motore esterno denominato "engine1" su SVM

vs1.example.com:

```
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: -
```

Crea eventi ONTAP FPolicy

Durante la creazione di una configurazione dei criteri FPolicy, è necessario creare un evento FPolicy. L'evento viene associato alla policy FPolicy al momento della sua creazione. Un evento definisce il protocollo da monitorare e gli eventi di accesso al file da monitorare e filtrare.

Prima di iniziare

È necessario completare l'evento FPolicy ["foglio di lavoro"](#).

Creare l'evento FPolicy

1. Creare l'evento FPolicy utilizzando `vserver fpolicy policy event create` comando.

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

2. Verificare la configurazione dell'evento FPolicy utilizzando `vserver fpolicy policy event show` comando.

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

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

Creare gli eventi di accesso negato FPolicy

A partire da ONTAP 9.13.1, gli utenti possono ricevere notifiche per operazioni di file non riuscite a causa della mancanza di autorizzazioni. Queste notifiche sono preziose per la sicurezza, la protezione ransomware e la governance.

1. Creare l'evento FPolicy utilizzando `vserver fpolicy policy event create` comando.

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

Crea archivi persistenti ONTAP FPolicy

Gli archivi persistenti possono aiutare a separare l'elaborazione i/o dei client dall'elaborazione delle notifiche FPolicy per ridurre la latenza dei client. A partire da ONTAP 9.14.1, FPolicy consente di configurare "[archivi persistenti](#)" Per acquisire eventi di accesso ai file per policy asincrone non obbligatorie nella SVM. Le configurazioni obbligatorie sincrone (obbligatorie o non obbligatorie) e asincrone non sono supportate.

A partire da ONTAP 9.15.1, la configurazione dell'archivio persistente di FPolicy è semplificata. Il `persistent-store create` Questo comando automatizza la creazione del volume per la SVM e configura il volume per l'archivio persistente.

Esistono due modi per creare un archivio permanente, a seconda della versione di ONTAP:

- ONTAP 9.15.1 o versione successiva: Quando si crea l'archivio persistente, ONTAP crea e configura automaticamente il proprio volume allo stesso tempo. Ciò semplifica la configurazione persistente dell'archivio FPolicy e implementa tutte le Best practice.
- ONTAP 9.14.1: Crea e configura manualmente un volume, quindi crea un archivio persistente per il volume appena creato.

È possibile configurare un solo archivio persistente per ciascuna SVM. Questo singolo archivio persistente deve essere utilizzato per tutte le configurazioni FPolicy su tale SVM, anche se le policy provengono da partner diversi.

Creare un archivio permanente (ONTAP 9.15.1 o versione successiva)

A partire da ONTAP 9.15.1, utilizzare `fpolicy persistent-store create` Comando per creare l'archivio persistente FPolicy con creazione e configurazione del volume inline. ONTAP blocca automaticamente il volume dall'accesso al protocollo utente esterno (CIFS/NFS).

Prima di iniziare

- La SVM in cui creare l'archivio persistente deve avere almeno un aggregato.
- Devi disporre dell'accesso agli aggregati disponibili per la SVM e di permessi sufficienti per creare i volumi.

Fasi

1. Creare l'archivio persistente, che crea e configura automaticamente il volume:

```
vserver fpolicy persistent-store create -vserver <vserver> -persistent-store <name> -volume <volume_name> -size <size> -autosize-mode
```

<off|grow|grow_shrink>

- Il **vserver** Parameter è il nome della SVM.
- Il **persistent-store** parametro è il nome dell'archivio permanente.
- Il **volume** parametro è il nome del volume di memorizzazione persistente.



Se si desidera utilizzare un volume vuoto esistente, utilizzare `volume show` per individuarlo e specificarlo nel parametro `volume`.

- Il **size** il parametro si basa sul tempo per il quale si desidera mantenere gli eventi che non vengono consegnati al server esterno (applicazione partner).

Ad esempio, se si desidera che 30 minuti di eventi persistano in un cluster con una capacità di 30K notifiche al secondo:

Dimensioni del volume richiesto = $30000 \times 30 \times 60 \times 0,6\text{KB}$ (dimensioni medie del record di notifica) = 32400000 KB = ~32 GB

Per trovare la percentuale approssimativa di notifica, è possibile contattare l'applicazione partner FPolicy o utilizzare il contatore `FPolicy requests_dispatched_rate`.



Se si utilizza un volume esistente, il parametro `size` è opzionale. Se si fornisce un valore per il parametro `size`, il volume verrà modificato con la dimensione specificata.

- Il **autosize-mode** parametro specifica la modalità di dimensionamento automatico del volume. Le modalità di dimensionamento automatico supportate sono:
 - Disattivato - il volume non aumenta o riduce le dimensioni in risposta alla quantità di spazio utilizzato.
 - Aumenta - il volume cresce automaticamente quando lo spazio utilizzato nel volume è al di sopra della soglia di crescita.
 - Grow_shrink - il volume cresce o si riduce in risposta alla quantità di spazio utilizzato.

2. Creare il criterio FPolicy e aggiungere il nome archivio permanente a tale criterio. Per ulteriori informazioni, vedere "[Creare il criterio FPolicy](#)".

Creare un archivio persistente (ONTAP 9.14.1)

Puoi creare un volume e quindi un archivio persistente per utilizzarlo. È possibile quindi bloccare il volume appena creato dall'accesso al protocollo utente esterno (CIFS/NFS).

Fasi

1. Creare un volume vuoto sulla SVM che può essere sottoposto a provisioning per l'archivio persistente:

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

Ci si aspetta che un utente amministratore con privilegi RBAC sufficienti (per creare un volume) crei un volume (utilizzando il comando cli di volume o l'API REST) della dimensione desiderata e fornisca il nome di quel volume come `-volume`. Nell'archivio persistente creare un comando CLI o API REST.

- Il `vserver` Parameter è il nome della SVM.
- Il `volume` parametro è il nome del volume di memorizzazione persistente.
- Il `state` il parametro deve essere impostato su `online` in modo che il volume sia disponibile per l'uso.
- Il `policy` Il parametro è impostato sulla politica di servizio FPolicy, se ne è già configurata una. In caso contrario, è possibile utilizzare `volume modify` in seguito, per aggiungere il criterio.
- Il `unix-permissions` il parametro è facoltativo.
- Il `size` il parametro si basa sul tempo per il quale si desidera mantenere gli eventi che non vengono consegnati al server esterno (applicazione partner).

Ad esempio, se si desidera che 30 minuti di eventi persistano in un cluster con una capacità di 30K notifiche al secondo:

Dimensioni del volume richiesto = $30000 \times 30 \times 60 \times 0,6\text{KB}$ (dimensioni medie del record di notifica) = 32400000 KB = ~32 GB

Per trovare la percentuale approssimativa di notifica, è possibile contattare l'applicazione partner FPolicy o utilizzare il contatore `FPolicy requests_dispatched_rate`.

- Il parametro `aggregate` è necessario per i volumi FlexVol, in caso contrario non è necessario.
- Il `snapshot-policy` il parametro deve essere impostato su `nessuno`. Ciò garantisce che non vi sia alcun ripristino accidentale dello snapshot che causa la perdita degli eventi correnti e impedisce l'elaborazione di eventuali duplicati degli eventi.

Se si desidera utilizzare un volume vuoto esistente, utilizzare `volume show` per trovarlo e l'`volume modify` per apportare le modifiche necessarie. Verificare il criterio, le dimensioni e la `snapshot-policy` i parametri sono impostati correttamente per l'archivio permanente.

2. Creare l'archivio persistente:

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

- Il `vserver` Parameter è il nome della SVM.
- Il `persistent-store` parametro è il nome dell'archivio permanente.
- Il `volume` parametro è il nome del volume di memorizzazione persistente.

3. Creare il criterio FPolicy e aggiungere il nome archivio permanente a tale criterio. Per ulteriori informazioni, vedere "["Creare il criterio FPolicy"](#).

Creare policy ONTAP FPolicy

Quando si crea il criterio FPolicy, si associa un motore esterno e uno o più eventi al criterio. Il criterio specifica inoltre se è richiesto lo screening obbligatorio, se i server FPolicy dispongono di un accesso privilegiato ai dati sulla macchina virtuale di storage (SVM) e se è attivata la funzione pass-through-Read per i file offline.

Prima di iniziare

- Il foglio di lavoro della policy FPolicy deve essere completato.

- Se si prevede di configurare il criterio per l'utilizzo dei server FPolicy, il motore esterno deve esistere.
- Deve esistere almeno un evento FPolicy che si prevede di associare al criterio FPolicy.
- Se si desidera configurare l'accesso privilegiato ai dati, è necessario che un server SMB esista sulla SVM.
- Per configurare un archivio persistente per un criterio, il tipo di motore deve essere **asincrono** e il criterio deve essere **non obbligatorio**.

Per ulteriori informazioni, vedere ["Creare archivi persistenti"](#).

Fasi

1. Creare la policy FPolicy:

```
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}]
```

- È possibile aggiungere uno o più eventi alla policy FPolicy.
- Per impostazione predefinita, lo screening obbligatorio è attivato.
- Se si desidera consentire l'accesso con privilegi impostando `-allow-privileged-access` parametro a. `yes`, è inoltre necessario configurare un nome utente con privilegi per l'accesso con privilegi.
- Se si desidera configurare pass-through-Read impostando `-is-passthrough-read-enabled` parametro a. `true`, è inoltre necessario configurare l'accesso privilegiato ai dati.

Il comando seguente crea una policy denominata "policy1" con l'evento "event1" e il motore esterno denominato "engine1" associato. Questo criterio utilizza i valori predefiniti nella configurazione del criterio: `vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

Il comando seguente crea una policy denominata "policy2" che ha l'evento "event2" e il motore esterno denominato "engine2" associato. Questo criterio è configurato per utilizzare l'accesso privilegiato utilizzando il nome utente specificato. La funzione di lettura pass-through è attivata:

```
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
```

Il comando seguente crea una policy denominata "native1" a cui è associato l'evento "event3". Questo criterio utilizza il motore nativo e i valori predefiniti nella configurazione del criterio:

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

2. Verificare la configurazione del criterio FPolicy utilizzando `vserver fpolicy policy show` comando.

Il seguente comando visualizza le informazioni relative ai tre criteri FPolicy configurati, incluse le seguenti informazioni:

- SVM associato al criterio

- Il motore esterno associato alla policy
- Gli eventi associati al criterio
- Se è richiesto lo screening obbligatorio
- Se è richiesto l'accesso con privilegi `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

Crea ambiti ONTAP FPolicy

Dopo aver creato il criterio FPolicy, è necessario creare un ambito FPolicy. Quando si crea l'ambito, si associa l'ambito a un criterio FPolicy. Un ambito definisce i limiti ai quali si applica la policy FPolicy. Gli ambiti possono includere o escludere file in base a condivisioni, policy di esportazione, volumi ed estensioni di file.

Prima di iniziare

Il foglio di lavoro FPolicy Scope deve essere completato. Il criterio FPolicy deve esistere con un motore esterno associato (se il criterio è configurato per l'utilizzo di server FPolicy esterni) e deve avere almeno un evento FPolicy associato.

Fasi

1. Creare l'ambito FPolicy utilizzando `vserver fpolicy policy scope create` comando.

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

2. Verificare la configurazione dell'ambito FPolicy utilizzando `vserver fpolicy policy scope show` comando.

```
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: -

```

Abilitare le policy ONTAP FPolicy

Dopo aver configurato una configurazione dei criteri FPolicy, si attiva il criterio FPolicy. L'abilitazione del criterio determina la priorità e avvia il monitoraggio dell'accesso al file per il criterio.

Prima di iniziare

Il criterio FPolicy deve esistere con un motore esterno associato (se il criterio è configurato per l'utilizzo di server FPolicy esterni) e deve avere almeno un evento FPolicy associato. L'ambito del criterio FPolicy deve esistere e deve essere assegnato al criterio FPolicy.

A proposito di questa attività

La priorità viene utilizzata quando sulla macchina virtuale di storage (SVM) sono attivati più criteri e più criteri sono stati sottoscritti allo stesso evento di accesso al file. I criteri che utilizzano la configurazione nativa del motore hanno una priorità maggiore rispetto ai criteri per qualsiasi altro motore, indipendentemente dal numero di sequenza assegnato al momento dell'attivazione del criterio.



Non è possibile attivare un criterio sulla SVM amministrativa.

Fasi

- Attivare il criterio FPolicy utilizzando `vserver fpolicy enable` comando.

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

- Verificare che il criterio FPolicy sia attivato utilizzando `vserver fpolicy show` comando.

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

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

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.