Pianificare la configurazione di FPolicy

ONTAP 9

NetApp
September 12, 2024

Sommario

Pianificare la configurazione di FPolicy . . . 1
Requisiti, considerazioni e Best practice per la configurazione di FPolicy . . . 1
Quali sono i passaggi per configurare una configurazione FPolicy . . . 7
Pianificare la configurazione del motore esterno FPolicy . . . 8
Pianificare la configurazione dell'evento FPolicy . . . 18
Pianificare la configurazione del criterio FPolicy . . . 28
Pianificare la configurazione dell'ambito FPolicy . . . 35

Pianificare la configurazione di FPolicy

Requisiti, considerazioni e Best practice per la configurazione di FPolicy

Prima di creare e configurare le configurazioni FPolicy sulle macchine virtuali dello storage (SVM), è necessario essere a conoscenza di determinati requisiti, considerazioni e Best practice per la configurazione di FPolicy.

Le funzionalità di FPolicy sono configurate tramite l'interfaccia a riga di comando (CLI) o tramite API REST.

Requisiti per la configurazione di FPolicy

Prima di configurare e abilitare FPolicy sulla macchina virtuale di storage (SVM), è necessario conoscere alcuni requisiti.

- Tutti i nodi del cluster devono eseguire una versione di ONTAP che supporti FPolicy.
- Se non si utilizza il motore FPolicy nativo di ONTAP, è necessario che siano installati server FPolicy esterni.
- I server FPolicy devono essere installati su un server accessibile dalle LIF dei dati di SVM in cui sono attivati i criteri FPolicy.

> A partire da ONTAP 9.8, ONTAP fornisce un servizio client LIF per connessioni FPolicy in uscita con l'aggiunta del `data-fpolicy-client` servizio. "Scopri di più sui LIF e sulle policy di servizio".

- L'indirizzo IP del server FPolicy deve essere configurato come server primario o secondario nella configurazione del motore esterno del criterio FPolicy.
- Se i server FPolicy accedono ai dati su un canale dati privilegiato, devono essere soddisfatti i seguenti requisiti aggiuntivi:
  - SMB deve essere concesso in licenza sul cluster.

    L'accesso privilegiato ai dati viene eseguito utilizzando connessioni SMB.
  - È necessario configurare una credenziale utente per accedere ai file sul canale dati privilegiato.
  - Il server FPolicy deve essere eseguito con le credenziali configurate nella configurazione FPolicy.
  - Tutti i dati LIF utilizzati per comunicare con i server FPolicy devono essere configurati in modo da avere `cifs` come uno dei protocolli consentiti.

    Sono inclusi i LIF utilizzati per le connessioni pass-through-Read.

Best practice e consigli per la configurazione di FPolicy

Durante la configurazione di FPolicy su macchine virtuali di storage (SVM), acquisire familiarità con le Best practice e i consigli generali per la configurazione di FPolicy per garantire performance di monitoraggio e risultati affidabili che soddisfino i requisiti.

Per le linee guida specifiche relative a performance, dimensionamento e configurazione, utilizzare

l'applicazione partner FPolicy.

Archivi persistenti

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

- Prima di utilizzare la funzionalità di archiviazione persistente, assicurarsi che le applicazioni partner supportino questa configurazione.
- Ti serve un archivio persistente per ogni SVM in cui è abilitato FPolicy.
  - 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.
- ONTAP 9.15.1 o versione successiva:
  - L'archivio persistente, il relativo volume e la relativa configurazione del volume vengono gestiti automaticamente quando si crea l'archivio persistente.
- ONTAP 9.14.1:
  - L'archivio persistente, il relativo volume e la relativa configurazione del volume vengono gestiti manualmente.
- Crea il volume di archivio persistente sul nodo con LIF che prevedono il monitoraggio del traffico massimo da parte di FPolicy.
  - ONTAP 9.15.1 o versioni successive: I volumi vengono creati e configurati automaticamente durante la creazione dell'archivio persistente.
  - ONTAP 9.14.1: Gli amministratori del cluster devono creare e configurare un volume per l'archivio persistente su ogni SVM dove è abilitato FPolicy.
- Se le notifiche accumulate nell'archivio permanente superano le dimensioni del volume fornito, FPolicy inizia a interrompere la notifica in arrivo con i messaggi EMS appropriati.
  - ONTAP 9.15.1 o versione successiva: In aggiunta al `size` , il `autosize-mode` parametro può aiutare il volume ad aumentare o ridurre in risposta alla quantità di spazio utilizzato.
  - ONTAP 9.14.1: Il `size` il parametro è configurato durante la creazione del volume per fornire un limite massimo.
- Impostare il criterio snapshot su `none` per il volume dell'archivio persistente invece di `default`. In questo modo si garantisce che non vi sia alcun ripristino accidentale dello snapshot che causa la perdita degli eventi correnti e per impedire un'eventuale elaborazione di eventi duplicati.
  - ONTAP 9.15.1 o versione successiva: Il `snapshot-policy` il parametro viene configurato automaticamente su nessuno durante la creazione dell'archivio permanente.
  - ONTAP 9.14.1: Il `snapshot-policy` il parametro è configurato su `none` durante la creazione del volume.
- Rendere il volume dell'archivio persistente inaccessibile per l'accesso al protocollo utente esterno (CIFS/NFS) per evitare il danneggiamento accidentale o l'eliminazione dei record di eventi persistenti.
  - ONTAP 9.15.1 o versioni successive: ONTAP blocca automaticamente il volume dall'accesso al protocollo utente esterno (CIFS/NFS) durante la creazione dell'archivio persistente.
  - ONTAP 9.14.1: Dopo aver attivato FPolicy, smontare il volume in ONTAP per rimuovere il percorso di giunzione. Questo lo rende inaccessibile per l'accesso ai protocolli utente esterni (CIFS/NFS).

Per ulteriori informazioni, fare riferimento a. "Archivi persistenti di FPolicy" e. "Creare archivi persistenti".

Failover e sconto del negozio persistente

L'archivio persistente rimane invariato quando è stato ricevuto l'ultimo evento, quando si verifica un riavvio imprevisto o FPolicy viene disattivato e riattivato. Dopo un'operazione di takeover, i nuovi eventi vengono memorizzati ed elaborati dal nodo partner. Dopo un'operazione di giveback, l'archivio persistente riprende l'elaborazione degli eventi non elaborati che potrebbero rimanere dal momento in cui si è verificato il takeover del nodo. Gli eventi live avrebbero la priorità rispetto agli eventi non elaborati.

Se il volume dell'archivio persistente si sposta da un nodo a un altro nella stessa SVM, le notifiche che non devono ancora essere elaborate vengono spostate anche nel nuovo nodo. È necessario eseguire nuovamente `fpolicy persistent-store create` su uno dei nodi dopo lo spostamento del volume, per garantire che le notifiche in sospeso vengano inviate al server esterno.

Configurazione dei criteri

La configurazione del motore esterno FPolicy, gli eventi e l'ambito per le SVM possono migliorare la tua esperienza e la sicurezza generale.

- Configurazione del motore esterno FPolicy per SVM:
  - Fornire una maggiore sicurezza implica un costo in termini di performance. L'abilitazione della comunicazione SSL (Secure Sockets Layer) ha un effetto sulle performance di accesso alle condivisioni.
  - Il motore esterno FPolicy deve essere configurato con più di un server FPolicy per garantire resilienza e alta disponibilità dell'elaborazione delle notifiche del server FPolicy.
- Configurazione degli eventi FPolicy per SVM:

  Il monitoraggio delle operazioni dei file influenza l'esperienza complessiva. Ad esempio, il filtraggio delle operazioni di file indesiderate sul lato dello storage migliora l'esperienza. NetApp consiglia di configurare la seguente configurazione:

  - Monitoraggio dei tipi minimi di operazioni di file e abilitazione del numero massimo di filtri senza interrompere il caso d'utilizzo.
  - Utilizzo di filtri per operazioni di getattr, lettura, scrittura, apertura e chiusura. Gli ambienti di home directory SMB e NFS hanno un'elevata percentuale di queste operazioni.
- Configurazione dell'ambito FPolicy per le SVM:

  Limitare l'ambito delle policy agli oggetti di storage rilevanti, come condivisioni, volumi ed esportazioni, invece di abilitarli nell'intera SVM. NetApp consiglia di controllare le estensioni di directory. Se il `is-file-extension-check-on-directories-enabled` il parametro è impostato su `true`, gli oggetti di directory sono sottoposti agli stessi controlli di estensione dei file normali.

Configurazione di rete

La connettività di rete tra il server FPolicy e il controller deve essere di bassa latenza. NetApp consiglia di separare il traffico FPolicy dal traffico client utilizzando una rete privata.

Inoltre, è necessario posizionare server FPolicy esterni (server FPolicy) nelle immediate vicinanze del cluster con connettività a elevata larghezza di banda per fornire una latenza minima e una connettività a elevata larghezza di banda.

> Per uno scenario in cui il traffico LIF per FPolicy viene configurato su una porta diversa da LIF per il traffico client, FPolicy LIF potrebbe eseguire il failover sull'altro nodo a causa di un errore della porta. Di conseguenza, il server FPolicy diventa irraggiungibile dal nodo, il che causa un errore nelle notifiche FPolicy per le operazioni sui file sul nodo. Per evitare questo problema, verificare che il server FPolicy possa essere raggiunto attraverso almeno un LIF sul nodo per elaborare le richieste FPolicy per le operazioni file eseguite su quel nodo.

Configurazione dell'hardware

Il server FPolicy può essere installato su un server fisico o virtuale. Se il server FPolicy si trova in un ambiente virtuale, è necessario allocare risorse dedicate (CPU, rete e memoria) al server virtuale.

Il rapporto nodo-server FPolicy del cluster deve essere ottimizzato per garantire che i server FPolicy non siano sovraccarichi, il che può introdurre latenze quando la SVM risponde alle richieste del client. Il rapporto ottimale dipende dall'applicazione del partner per cui viene utilizzato il server FPolicy. NetApp consiglia di collaborare con i partner per determinare il valore appropriato.

Configurazione a più policy

La policy FPolicy per il blocco nativo ha la priorità più alta, indipendentemente dal numero di sequenza, e le policy di modifica delle decisioni hanno una priorità più alta rispetto ad altre. La priorità della policy dipende dal caso d'utilizzo. NetApp consiglia di collaborare con i partner per determinare la priorità appropriata.

Considerazioni sulle dimensioni

FPolicy esegue il monitoraggio in linea delle operazioni SMB e NFS, invia notifiche al server esterno e attende una risposta, a seconda della modalità di comunicazione esterna del motore (sincrona o asincrona). Questo processo influisce sulle prestazioni dell'accesso SMB e NFS e sulle risorse della CPU.

Per mitigare eventuali problemi, NetApp consiglia di collaborare con i partner per valutare e dimensionare l'ambiente prima di abilitare FPolicy. Le performance sono influenzate da diversi fattori, tra cui il numero di utenti, le caratteristiche dei carichi di lavoro, come le operazioni per utente e le dimensioni dei dati, la latenza di rete e la lentezza dei guasti o dei server.

Monitorare le performance

FPolicy è un sistema basato su notifiche. Le notifiche vengono inviate a un server esterno per l'elaborazione e la generazione di una risposta a ONTAP. Questo processo di andata e ritorno aumenta la latenza per l'accesso al client.

Il monitoraggio dei contatori delle performance sul server FPolicy e in ONTAP consente di identificare i colli di bottiglia nella soluzione e di ottimizzare i parametri in base alle necessità per una soluzione ottimale. Ad esempio, un aumento della latenza di FPolicy ha un effetto a cascata sulla latenza di accesso SMB e NFS. Pertanto, è necessario monitorare sia il carico di lavoro (SMB e NFS) che la latenza di FPolicy. Inoltre, è possibile utilizzare le policy di qualità del servizio in ONTAP per impostare un carico di lavoro per ogni volume o SVM abilitato per FPolicy.

NetApp consiglia di eseguire `statistics show -object workload` per visualizzare le statistiche del carico di lavoro. Inoltre, è necessario monitorare i seguenti parametri:

- Latenze medie, di lettura e di scrittura
- Numero totale di operazioni
- Contatori di lettura e scrittura

È possibile monitorare le performance dei sottosistemi FPolicy utilizzando i seguenti contatori FPolicy.

> Per raccogliere le statistiche relative a FPolicy, è necessario essere in modalità diagnostica.

Fasi

1. Raccogliere i contatori FPolicy:
   a. `statistics start -object fpolicy -instance` *`instance_name`* `-sample-id` *`ID`*
   b. `statistics start -object fpolicy_policy -instance` *`instance_name`* `-sample-id` *`ID`*
2. Visualizza contatori FPolicy:
   a. `statistics show -object fpolicy –instance` *`instance_name`* `-sample-id` *`ID`*
   b. `statistics show -object fpolicy_server –instance` *`instance_name`* `-sample-id` *`ID`*

   Il `fpolicy` e. `fpolicy_server` i contatori forniscono informazioni su diversi parametri delle prestazioni descritti nella tabella seguente.

Contatori	Descrizione
• contatori "fpolicy"*	richieste_interrotte
Numero di richieste sullo schermo per le quali l'elaborazione viene interrotta sulla SVM	conteggio_eventi
Elenco degli eventi risultanti dalla notifica	latenza_richiesta_massima
Latenza massima richiesta dallo schermo	richieste_in sospeso
Numero totale di richieste di schermate in corso	processed_requests
Numero totale di richieste eseguite tramite l'elaborazione di fpolicy nella SVM	request_latency_hist
Istogramma della latenza per le richieste dello schermo	requests_dispatched_rate
Numero di richieste di videata inviate al secondo	requests_received_rate
Numero di richieste di videata ricevute al secondo	• contatori "fpolicy_server"*
latenza_richiesta_massima	Latenza massima per una richiesta dello schermo

Contatori	Descrizione
richieste_in sospeso	Numero totale di richieste sullo schermo in attesa di risposta
request_latency	Latenza media per la richiesta dello schermo
request_latency_hist	Istogramma della latenza per le richieste dello schermo
request_sent_rate	Numero di screen request inviate al server FPolicy al secondo
response_received_rate	Numero di risposte sullo schermo ricevute dal server FPolicy al secondo

Gestire il workflow FPolicy e la dipendenza da altre tecnologie

NetApp consiglia di disattivare un criterio FPolicy prima di apportare modifiche alla configurazione. Ad esempio, se si desidera aggiungere o modificare un indirizzo IP nel motore esterno configurato per il criterio Enabled (attivato), disattivare prima il criterio.

Se si configura FPolicy per il monitoraggio dei volumi NetApp FlexCache, NetApp consiglia di non configurare FPolicy per monitorare le operazioni di lettura e getattr dei file. Il monitoraggio di queste operazioni in ONTAP richiede il recupero dei dati inode-to-path (I2P). Poiché i dati I2P non possono essere recuperati dai volumi FlexCache, devono essere recuperati dal volume di origine. Pertanto, il monitoraggio di queste operazioni elimina i benefici in termini di performance che FlexCache può offrire.

Quando vengono implementate sia FPolicy che una soluzione antivirus off-box, la soluzione antivirus riceve prima le notifiche. L'elaborazione di FPolicy viene avviata solo al termine della scansione antivirus. È importante dimensionare correttamente le soluzioni antivirus perché un programma antivirus lento può influire sulle prestazioni generali.

Considerazioni su upgrade e revert in lettura passthrough

Prima di eseguire l'aggiornamento a una release di ONTAP che supporta la lettura pass-through o prima di tornare a una release che non supporta la lettura pass-through, è necessario conoscere alcune considerazioni relative all'aggiornamento e al ripristino.

Aggiornamento in corso

Dopo l'aggiornamento di tutti i nodi a una versione di ONTAP che supporta FPolicy pass-through-Read, il cluster è in grado di utilizzare la funzionalità pass-through-Read; tuttavia, il pass-through-Read viene disattivato per impostazione predefinita nelle configurazioni FPolicy esistenti. Per utilizzare pass-through-Read sulle configurazioni FPolicy esistenti, è necessario disattivare il criterio FPolicy e modificare la configurazione, quindi riattivarla.

In corso

Prima di ripristinare una versione di ONTAP che non supporta FPolicy pass-through-Read, è necessario soddisfare le seguenti condizioni:

- Disattivare tutti i criteri utilizzando pass-through-Read, quindi modificare le configurazioni interessate in modo che non utilizzino pass-through-Read.
- Disattivare la funzionalità FPolicy sul cluster disattivando tutti i criteri FPolicy sul cluster.

Prima di tornare a una versione di ONTAP che non supporta gli archivi persistenti, assicurarsi che nessuno dei criteri FPolicy disponga di un archivio persistente configurato. Se è configurato un archivio persistente, l'indirizzamento non riesce.

Quali sono i passaggi per configurare una configurazione FPolicy

Prima che FPolicy possa monitorare l'accesso ai file, è necessario creare e abilitare una configurazione FPolicy sulla macchina virtuale di storage (SVM) per la quale sono richiesti i servizi FPolicy.

Di seguito sono riportati i passaggi per impostare e abilitare una configurazione FPolicy su SVM:

1. Creare un motore esterno FPolicy.

   Il motore esterno FPolicy identifica i server FPolicy esterni (server FPolicy) associati a una specifica configurazione FPolicy. Se il motore FPolicy interno "nativo" viene utilizzato per creare una configurazione di blocco dei file nativa, non è necessario creare un motore esterno FPolicy.

   A partire da ONTAP 9.15.1, è possibile utilizzare `protobuf` formato motore. Quando è impostato su `protobuf`, I messaggi di notifica sono codificati in forma binaria utilizzando Google Protobuf. Prima di impostare il formato del motore su `protobuf`, Verificare che anche il server FPolicy supporti `protobuf` deserializzazione. Per ulteriori informazioni, vedere "Pianificare la configurazione del motore esterno FPolicy"

2. Creare un evento FPolicy.

   Un evento FPolicy descrive ciò che la policy FPolicy deve monitorare. Gli eventi sono costituiti dai protocolli e dalle operazioni dei file da monitorare e possono contenere un elenco di filtri. Gli eventi utilizzano filtri per limitare l'elenco degli eventi monitorati per i quali il motore esterno FPolicy deve inviare notifiche. Gli eventi specificano anche se il criterio monitora le operazioni del volume.

3. Creare un archivio permanente FPolicy (opzionale).

   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.

   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 9.15.1, 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.

4. Creare una policy FPolicy.

   Il criterio FPolicy è responsabile dell'associazione, con l'ambito appropriato, dell'insieme di eventi da monitorare e per i quali le notifiche degli eventi monitorati devono essere inviate al server FPolicy designato (o al motore nativo se non sono configurati server FPolicy). Il criterio definisce inoltre se al server FPolicy è consentito l'accesso privilegiato ai dati per i quali riceve le notifiche. Un server FPolicy ha bisogno di un accesso privilegiato se il server ha bisogno di accedere ai dati. I casi di utilizzo tipici in cui è necessario un accesso privilegiato includono il blocco dei file, la gestione delle quote e la gestione dello storage gerarchico. Il criterio consente di specificare se la configurazione di questo criterio utilizza un server FPolicy o il server FPolicy interno "nativo".

   Un criterio specifica se lo screening è obbligatorio. Se lo screening è obbligatorio e tutti i server FPolicy non sono attivi o non viene ricevuta alcuna risposta dai server FPolicy entro un periodo di timeout definito,

l'accesso al file viene negato.

I limiti di una policy sono la SVM. Un criterio non può essere applicato a più di una SVM. Tuttavia, una SVM specifica può avere più policy FPolicy, ciascuna con la stessa o diversa combinazione di ambito, evento e configurazioni di server esterni.

5. Configurare l'ambito del criterio.

   L'ambito di FPolicy determina i volumi, le condivisioni o le policy di esportazione su cui la policy agisce o esclude dal monitoraggio. Un ambito determina anche quali estensioni di file devono essere incluse o escluse dal monitoraggio di FPolicy.

   Gli elenchi di esclusione hanno la precedenza sugli elenchi di inclusione.

6. Attivare il criterio FPolicy.

   Quando il criterio è attivato, i canali di controllo e, facoltativamente, i canali dati privilegiati sono connessi. Il processo FPolicy sui nodi a cui partecipa SVM inizia a monitorare l'accesso a file e cartelle e, per gli eventi che corrispondono ai criteri configurati, invia notifiche ai server FPolicy (o al motore nativo se non sono configurati server FPolicy).

Se il criterio utilizza il blocco dei file nativi, un motore esterno non viene configurato o associato al criterio.

Pianificare la configurazione del motore esterno FPolicy

Pianificare la configurazione del motore esterno FPolicy

Prima di configurare il motore esterno FPolicy, è necessario comprendere cosa significa creare un motore esterno e quali parametri di configurazione sono disponibili. Queste informazioni consentono di determinare i valori da impostare per ciascun parametro.

Informazioni definite durante la creazione del motore esterno FPolicy

La configurazione del motore esterno definisce le informazioni necessarie a FPolicy per creare e gestire le connessioni ai server FPolicy esterni, tra cui:

- Nome SVM
- Nome del motore
- Gli indirizzi IP dei server FPolicy primario e secondario e il numero di porta TCP da utilizzare per la connessione ai server FPolicy
- Se il tipo di motore è asincrono o sincrono
- Se il formato del motore è `xml` oppure `protobuf`

  A partire da ONTAP 9.15.1, è possibile utilizzare `protobuf` formato motore. Quando è impostato su `protobuf`, I messaggi di notifica sono codificati in forma binaria utilizzando Google Protobuf. Prima di impostare il formato del motore su `protobuf`, Verificare che anche il server FPolicy supporti `protobuf` deserializzazione.

  Poiché il formato protobuf è supportato a partire da ONTAP 9.15.1, è necessario considerare il formato del

motore esterno prima di tornare a una versione precedente di ONTAP. Se si torna a una versione precedente rispetto a ONTAP 9.15.1, collaborare con il partner FPolicy per:

  - Modificare ogni formato del motore da `protobuf` a. `xml`
  - Eliminare i motori con un formato motore di `protobuf`

- Come autenticare la connessione tra il nodo e il server FPolicy

  Se si sceglie di configurare l'autenticazione SSL reciproca, è necessario configurare anche i parametri che forniscono le informazioni del certificato SSL.

- Come gestire la connessione utilizzando diverse impostazioni avanzate dei privilegi

  Sono inclusi parametri che definiscono valori di timeout, valori di tentativi, valori di mantenimento, valori di richiesta massimi, valori di dimensione buffer inviati e ricevuti e valori di timeout della sessione.

Il `vserver fpolicy policy external-engine create` Il comando viene utilizzato per creare un motore esterno FPolicy.

Quali sono i parametri esterni di base del motore

È possibile utilizzare la seguente tabella dei parametri di configurazione di base di FPolicy per pianificare la configurazione:

Tipo di informazione	Opzione
SVM Specifica il nome SVM che si desidera associare a questo motore esterno. Ogni configurazione FPolicy viene definita all'interno di una singola SVM. Il motore esterno, l'evento del criterio, l'ambito del criterio e il criterio che si combinano insieme per creare una configurazione del criterio FPolicy devono essere tutti associati alla stessa SVM.	`-vserver` `vserver_name`

Nome motore Specifica il nome da assegnare alla configurazione esterna del motore. È necessario specificare il nome del motore esterno in un secondo momento quando si crea il criterio FPolicy. In questo modo, il motore esterno viene associato alla policy. Il nome può contenere fino a 256 caratteri. Se si configura il nome del motore esterno in una configurazione di disaster recovery MetroCluster o SVM, il nome deve essere composto da un massimo di 200 caratteri. Il nome può contenere qualsiasi combinazione dei seguenti caratteri ASCII: • `a` attraverso `z` • `A` attraverso `Z` • `0` attraverso `9` • “_”, “-”, and "``"	`-engine-name engine_name`
Server FPolicy primari Specifica i server FPolicy primari a cui il nodo invia le notifiche per un dato criterio FPolicy. Il valore viene specificato come elenco di indirizzi IP delimitato da virgole. Se viene specificato più di un indirizzo IP del server primario, ogni nodo a cui partecipa SVM crea una connessione di controllo a ogni server FPolicy primario specificato al momento dell’attivazione del criterio. Se si configurano più server FPolicy primari, le notifiche vengono inviate ai server FPolicy in modo round-robin. Se il motore esterno viene utilizzato in una configurazione di disaster recovery MetroCluster o SVM, 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.	`-primary-servers IP_address,...`
Numero porta Specifica il numero di porta del servizio FPolicy.	`-port integer`

Server FPolicy secondari Specifica i server FPolicy secondari a cui inviare gli eventi di accesso ai file per un determinato criterio FPolicy. Il valore viene specificato come elenco di indirizzi IP delimitato da virgole. I server secondari vengono utilizzati solo quando nessuno dei server primari è raggiungibile. Le connessioni ai server secondari vengono stabilite quando il criterio è attivato, ma le notifiche vengono inviate ai server secondari solo se nessuno dei server primari è raggiungibile. Se si configurano più server secondari, le notifiche vengono inviate ai server FPolicy in modo round-robin.	`-secondary-servers IP_address,...`
Tipo di motore esterno Specifica se il motore esterno funziona in modalità sincrona o asincrona. Per impostazione predefinita, FPolicy opera in modalità sincrona. Quando è impostato su `synchronous`, L'elaborazione della richiesta di file invia una notifica al server FPolicy, ma non continua fino a quando non riceve una risposta dal server FPolicy. A questo punto, il flusso della richiesta continua o l'elaborazione comporta un rifiuto, a seconda che la risposta dal server FPolicy consenta l'azione richiesta. Quando è impostato su `asynchronous`, L'elaborazione della richiesta di file invia una notifica al server FPolicy, quindi continua.	`-extern-engine-type external_engine_type` Il valore di questo parametro può essere uno dei seguenti: • `synchronous` • `asynchronous`
Formato motore esterno Specificare se il formato del motore esterno è xml o protobuf. A partire da ONTAP 9.15.1, è possibile utilizzare il formato del motore protobuf. Quando è impostato su protobuf, i messaggi di notifica vengono codificati in formato binario utilizzando Google Protobuf. Prima di impostare il formato del motore su protobuf, verificare che il server FPolicy supporti anche la deserializzazione di protobuf.	`- extern-engine-format` {`protobuf` oppure `xml`}

Opzione SSL per la comunicazione con il server FPolicy Specifica l'opzione SSL per la comunicazione con il server FPolicy. Questo è un parametro obbligatorio. È possibile scegliere una delle opzioni in base alle seguenti informazioni: • Quando è impostato su `no-auth`, non viene eseguita alcuna autenticazione. Il collegamento di comunicazione viene stabilito tramite TCP. • Quando è impostato su `server-auth`, SVM autentica il server FPolicy utilizzando l'autenticazione del server SSL. • Quando è impostato su `mutual-auth`, L'autenticazione reciproca avviene tra SVM e il server FPolicy; SVM autentica il server FPolicy e il server FPolicy autentica SVM. Se si sceglie di configurare l'autenticazione SSL reciproca, è necessario configurare anche `-certificate-common-name`, `-certificate -serial`, e. `-certifcate-ca` parametri.	`-ssl-option` {`no-auth`
`server-auth`	`mutual-auth`}
FQDN certificato o nome comune personalizzato Specifica il nome del certificato utilizzato se è configurata l'autenticazione SSL tra SVM e il server FPolicy. È possibile specificare il nome del certificato come FQDN o come nome comune personalizzato. Se si specifica `mutual-auth` per `-ssl-option` specificare un valore per `-certificate-common-name` parametro.	`-certificate-common -name` `text`
Numero di serie del certificato Specifica il numero di serie del certificato utilizzato per l'autenticazione se è configurata l'autenticazione SSL tra SVM e il server FPolicy. Se si specifica `mutual-auth` per `-ssl-option` specificare un valore per `-certificate-serial` parametro.	`-certificate-serial` `text`
Autorità di certificazione Specifica il nome della CA del certificato utilizzato per l'autenticazione se è configurata l'autenticazione SSL tra SVM e il server FPolicy. Se si specifica `mutual-auth` per `-ssl-option` specificare un valore per `-certificate-ca` parametro.	`-certificate-ca` `text`

Quali sono le opzioni avanzate dei motori esterni

È possibile utilizzare la seguente tabella di parametri di configurazione FPolicy avanzati quando si prevede di

personalizzare la configurazione con parametri avanzati. Questi parametri vengono utilizzati per modificare il comportamento delle comunicazioni tra i nodi del cluster e i server FPolicy:

Tipo di informazione	Opzione
Timeout per l'annullamento di una richiesta Specifica l'intervallo di tempo in ore (`h`), minuti (`m`), o secondi (`s`) Che il nodo attende una risposta dal server FPolicy. Se l'intervallo di timeout viene superato, il nodo invia una richiesta di annullamento al server FPolicy. Il nodo invia quindi la notifica a un server FPolicy alternativo. Questo timeout consente di gestire un server FPolicy che non risponde, migliorando la risposta del client SMB/NFS. Inoltre, l'annullamento delle richieste dopo un periodo di timeout può aiutare a rilasciare le risorse di sistema perché la richiesta di notifica viene spostata da un server FPolicy inattivo/non funzionante a un server FPolicy alternativo. L'intervallo per questo valore è `0` attraverso `100`. Se il valore è impostato su `0`, L'opzione è disattivata e i messaggi di richiesta di annullamento non vengono inviati al server FPolicy. L'impostazione predefinita è `20s`.	`-reqs-cancel-timeout integer`[h
m	s]
Timeout per l'interruzione di una richiesta Specifica il timeout in ore (`h`), minuti (`m`), o secondi (`s`) per interrompere una richiesta. L'intervallo per questo valore è `0` attraverso `200`.	`-reqs-abort-timeout` ` `integer`[h
m	s]
Intervallo per l'invio delle richieste di stato Specifica l'intervallo in ore (`h`), minuti (`m`), o secondi (`s`) Dopo di che viene inviata una richiesta di stato al server FPolicy. L'intervallo per questo valore è `0` attraverso `50`. Se il valore è impostato su `0`, L'opzione è disattivata e i messaggi di richiesta di stato non vengono inviati al server FPolicy. L'impostazione predefinita è `10s`.	`-status-req-interval integer`[h
m	s]
Numero massimo di richieste in sospeso sul server FPolicy Specifica il numero massimo di richieste in sospeso che è possibile mettere in coda sul server FPolicy. L'intervallo per questo valore è `1` attraverso `10000`. L'impostazione predefinita è `500`.	`-max-server-reqs integer`

Timeout per la disconnessione di un server FPolicy che non risponde Specifica l'intervallo di tempo in ore (`h`), minuti (`m`), o secondi (`s`) Dopo di che la connessione al server FPolicy viene interrotta. La connessione viene interrotta dopo il periodo di timeout solo se la coda del server FPolicy contiene il numero massimo consentito di richieste e non viene ricevuta alcuna risposta entro il periodo di timeout. Il numero massimo consentito di richieste è `50` (impostazione predefinita) o il numero specificato da `max-server-reqs-` parametro. L'intervallo per questo valore è `1` attraverso `100`. L'impostazione predefinita è `60s`.	`-server-progress -timeout integer`[h
m	s]
Intervallo per l'invio di messaggi keep-alive al server FPolicy Specifica l'intervallo di tempo in ore (`h`), minuti (`m`), o secondi (`s`) In cui i messaggi keep-alive vengono inviati al server FPolicy. I messaggi keep-alive rilevano connessioni half-open. L'intervallo per questo valore è `10` attraverso `600`. Se il valore è impostato su `0`, L'opzione è disattivata e non è possibile inviare messaggi keep-alive ai server FPolicy. L'impostazione predefinita è `120s`.	`-keep-alive-interval- integer`[h
m	s]
Numero massimo di tentativi di riconnessione Specifica il numero massimo di tentativi di riconnessione da parte di SVM al server FPolicy dopo l'interruzione della connessione. L'intervallo per questo valore è `0` attraverso `20`. L'impostazione predefinita è `5`.	`-max-connection-retries integer`
Dimensione buffer di ricezione Specifica la dimensione del buffer di ricezione del socket connesso per il server FPolicy. Il valore predefinito è 256 kilobyte (Kb). Quando il valore è impostato su 0, la dimensione del buffer di ricezione viene impostata su un valore definito dal sistema. Ad esempio, se la dimensione predefinita del buffer di ricezione del socket è 65536 byte, impostando il valore sintonizzabile su 0, la dimensione del buffer del socket viene impostata su 65536 byte. È possibile utilizzare qualsiasi valore non predefinito per impostare la dimensione (in byte) del buffer di ricezione.	`-recv-buffer-size integer`

Invia dimensione buffer Specifica la dimensione del buffer di invio del socket connesso per il server FPolicy. Il valore predefinito è 256 kilobyte (Kb). Quando il valore è impostato su 0, la dimensione del buffer di invio viene impostata su un valore definito dal sistema. Ad esempio, se la dimensione predefinita del buffer di invio del socket è impostata su 65536 byte, impostando il valore sintonizzabile su 0, la dimensione del buffer del socket viene impostata su 65536 byte. È possibile utilizzare qualsiasi valore non predefinito per impostare la dimensione (in byte) del buffer di invio.	`-send-buffer-size integer`
Timeout per l'eliminazione di un ID sessione durante la riconnessione Specifica l'intervallo in ore (`h`), minuti (`m`), o secondi (`s`) Dopo di che viene inviato un nuovo ID di sessione al server FPolicy durante i tentativi di riconnessione. Se la connessione tra il controller di storage e il server FPolicy viene interrotta e la riconnessione viene effettuata all'interno di `-session -timeout` Intervallo, il vecchio ID sessione viene inviato al server FPolicy in modo che possa inviare le risposte per le vecchie notifiche. Il valore predefinito è impostato su 10 secondi.	`-session-timeout` [`.integer`h][`integer`m][`integer`s]

Ulteriori informazioni sulla configurazione dei motori esterni FPolicy per l'utilizzo di connessioni autenticate SSL

Per configurare il motore esterno FPolicy in modo che utilizzi SSL durante la connessione ai server FPolicy, è necessario conoscere alcune informazioni aggiuntive.

Autenticazione del server SSL

Se si sceglie di configurare il motore esterno FPolicy per l'autenticazione del server SSL, prima di creare il motore esterno, è necessario installare il certificato pubblico dell'autorità di certificazione (CA) che ha firmato il certificato del server FPolicy.

Autenticazione reciproca

Se si configurano i motori esterni di FPolicy in modo che utilizzino l'autenticazione reciproca SSL quando si collegano i LIF dei dati delle macchine virtuali di storage (SVM) ai server FPolicy esterni, prima di creare il motore esterno, È necessario installare il certificato pubblico della CA che ha firmato il certificato del server FPolicy insieme al certificato pubblico e al file delle chiavi per l'autenticazione della SVM. Non è necessario eliminare questo certificato mentre i criteri FPolicy utilizzano il certificato installato.

Se il certificato viene eliminato mentre FPolicy lo utilizza per l'autenticazione reciproca durante la connessione a un server FPolicy esterno, non è possibile riabilitare un criterio FPolicy disattivato che utilizza tale certificato. Non è possibile riabilitare il criterio FPolicy in questa situazione anche se viene creato e installato un nuovo certificato con le stesse impostazioni sulla SVM.

Se il certificato è stato eliminato, è necessario installare un nuovo certificato, creare nuovi motori esterni FPolicy che utilizzano il nuovo certificato e associare i nuovi motori esterni al criterio FPolicy che si desidera riabilitare modificando il criterio FPolicy.

Installare i certificati per SSL

Il certificato pubblico della CA utilizzato per firmare il certificato del server FPolicy viene installato utilizzando `security certificate install` con il `-type` parametro impostato su `client-ca`. La chiave privata e il certificato pubblico richiesti per l'autenticazione della SVM vengono installati utilizzando `security certificate install` con il `-type` parametro impostato su `server`.

I certificati non vengono replicati nelle relazioni di disaster recovery SVM con una configurazione non-ID-preserve

I certificati di sicurezza utilizzati per l'autenticazione SSL durante le connessioni ai server FPolicy non replicano nelle destinazioni di disaster recovery SVM con configurazioni non ID-preserve. Sebbene la configurazione del motore esterno FPolicy sulla SVM sia replicata, i certificati di sicurezza non vengono replicati. È necessario installare manualmente i certificati di protezione sulla destinazione.

Quando si imposta la relazione di disaster recovery SVM, il valore selezionato per `-identity-preserve` opzione di `snapmirror create` Determina i dettagli di configurazione replicati nella SVM di destinazione.

Se si imposta `-identity-preserve` opzione a. `true` (ID-Preserve), vengono replicati tutti i dettagli di configurazione di FPolicy, incluse le informazioni del certificato di sicurezza. È necessario installare i certificati di protezione sulla destinazione solo se si imposta l'opzione su `false` (Non-ID-Preserve).

Restrizioni per motori esterni FPolicy con ambito cluster con configurazioni di disaster recovery MetroCluster e SVM

È possibile creare un motore esterno FPolicy con ambito cluster assegnando la SVM (Cluster Storage Virtual Machine) al motore esterno. Tuttavia, quando si crea un motore esterno con ambito cluster in una configurazione di disaster recovery MetroCluster o SVM, esistono alcune restrizioni quando si sceglie il metodo di autenticazione utilizzato da SVM per la comunicazione esterna con il server FPolicy.

Quando si creano server FPolicy esterni, è possibile scegliere tre opzioni di autenticazione: Nessuna autenticazione, autenticazione del server SSL e autenticazione reciproca SSL. Sebbene non vi siano restrizioni quando si sceglie l'opzione di autenticazione se il server FPolicy esterno è assegnato a una SVM di dati, esistono restrizioni quando si crea un motore esterno FPolicy con ambito cluster:

Configurazione	Consentito?
Disaster recovery MetroCluster o SVM e motore esterno FPolicy con ambito cluster senza autenticazione (SSL non configurato)	Sì
Disaster recovery MetroCluster o SVM e motore esterno FPolicy con ambito cluster con server SSL o autenticazione reciproca SSL	No

- Se esiste un motore esterno FPolicy con ambito cluster con autenticazione SSL e si desidera creare una configurazione di disaster recovery MetroCluster o SVM, è necessario modificare questo motore esterno in modo che non utilizzi alcuna autenticazione o rimuovere il motore esterno prima di poter creare la configurazione di disaster recovery MetroCluster o SVM.
- Se la configurazione di disaster recovery MetroCluster o SVM esiste già, ONTAP impedisce di creare un motore esterno FPolicy con ambito cluster e autenticazione SSL.

Completare il foglio di lavoro di configurazione del motore esterno FPolicy

È possibile utilizzare questo foglio di lavoro per registrare i valori necessari durante il processo di configurazione del motore esterno FPolicy. Se è richiesto un valore di parametro, è necessario determinare quale valore utilizzare per tali parametri prima di configurare il motore esterno.

Informazioni per una configurazione di base del motore esterno

Registrare se si desidera includere ogni impostazione di parametro nella configurazione esterna del motore e quindi registrare il valore dei parametri che si desidera includere.

Tipo di informazione	Obbligatorio	Includi	I tuoi valori
Nome SVM (Storage Virtual Machine)	Sì	Sì	
Nome del motore	Sì	Sì	
Server FPolicy primari	Sì	Sì	
Numero di porta	Sì	Sì	
Server FPolicy secondari	No		
Tipo di motore esterno	No		
Opzione SSL per la comunicazione con il server FPolicy esterno	Sì	Sì	
FQDN certificato o nome comune personalizzato	No		
Numero di serie del certificato	No		
Autorità di certificazione	No		

Informazioni sui parametri esterni avanzati del motore

Per configurare un motore esterno con parametri avanzati, è necessario immettere il comando di configurazione in modalità avanzata con privilegi.

Tipo di informazione	Obbligatorio	Includi	I tuoi valori
Timeout per l'annullamento di una richiesta	No		
Timeout per l'interruzione di una richiesta	No		
Intervallo per l'invio delle richieste di stato	No		
Numero massimo di richieste in sospeso sul server FPolicy	No		
Timeout per la disconnessione di un server FPolicy che non risponde	No		
Intervallo per l'invio di messaggi keep-alive al server FPolicy	No		
Numero massimo di tentativi di riconnessione	No		
Dimensione buffer di ricezione	No		
Dimensione buffer di invio	No		
Timeout per l'eliminazione di un ID sessione durante la riconnessione	No		

Pianificare la configurazione dell'evento FPolicy

Pianificare la panoramica della configurazione degli eventi FPolicy

Prima di configurare gli eventi FPolicy, è necessario comprendere il significato di creazione di un evento FPolicy. È necessario determinare quali protocolli si desidera monitorare l'evento, quali eventi monitorare e quali filtri eventi utilizzare. Queste informazioni consentono di pianificare i valori che si desidera impostare.

Cosa significa creare un evento FPolicy

La creazione dell'evento FPolicy implica la definizione delle informazioni necessarie al processo FPolicy per determinare quali operazioni di accesso ai file monitorare e per quali notifiche degli eventi monitorati devono essere inviate al server FPolicy esterno. La configurazione degli eventi FPolicy definisce le seguenti informazioni di configurazione:

- Nome SVM (Storage Virtual Machine)
- Nome dell'evento
- Quali protocolli monitorare

FPolicy può monitorare le operazioni di accesso ai file SMB, NFSv3, NFSv4 e, a partire da ONTAP 9.15.1, NFSv4,1.

- Quali operazioni di file monitorare

  Non tutte le operazioni sui file sono valide per ciascun protocollo.

- Quali filtri di file configurare

  Sono valide solo alcune combinazioni di operazioni e filtri dei file. Ogni protocollo dispone di un proprio set di combinazioni supportate.

- Se monitorare le operazioni di montaggio e smontaggio del volume

> Esiste una dipendenza con tre parametri (`-protocol`, `-file-operations`, `-filters`). Le seguenti combinazioni sono valide per i tre parametri:
>
> - È possibile specificare `-protocol` e. `-file-operations` parametri.
> - È possibile specificare tutti e tre i parametri.
> - Non è possibile specificare alcun parametro.

Contenuto della configurazione dell'evento FPolicy

È possibile utilizzare il seguente elenco di parametri di configurazione degli eventi FPolicy disponibili per pianificare la configurazione:

Tipo di informazione	Opzione
SVM Specifica il nome SVM che si desidera associare a questo evento FPolicy. Ogni configurazione FPolicy viene definita all'interno di una singola SVM. Il motore esterno, l'evento del criterio, l'ambito del criterio e il criterio che si combinano insieme per creare una configurazione del criterio FPolicy devono essere tutti associati alla stessa SVM.	`-vserver vserver_name`

Nome evento Specifica il nome da assegnare all'evento FPolicy. Quando si crea il criterio FPolicy, l'evento FPolicy viene associato al criterio utilizzando il nome dell'evento. Il nome può contenere fino a 256 caratteri. Se si configura l'evento in una configurazione di disaster recovery MetroCluster o SVM, il nome deve contenere fino a 200 caratteri. Il nome può contenere qualsiasi combinazione dei seguenti caratteri ASCII: • `a` attraverso `z` • `A` attraverso `Z` • `0` attraverso `9` • " _ ", "-", and "``"	`-event-name` `event_name`
Protocollo Specifica quale protocollo configurare per l'evento FPolicy. L'elenco per `-protocol` può includere uno dei seguenti valori: • `cifs` • `nfsv3` • `nfsv4` Se si specifica `-protocol`, quindi specificare un valore valido in `-file-operations` parametro. Man mano che la versione del protocollo cambia, i valori validi potrebbero cambiare. A partire da ONTAP 9.15.1, NFSv4 consente di acquisire eventi NFSv4,0 e NFSv4,1.	`-protocol` `protocol`

Operazioni file Specifica l'elenco delle operazioni del file per l'evento FPolicy. L'evento controlla le operazioni specificate in questo elenco da tutte le richieste client utilizzando il protocollo specificato in `-protocol` parametro. È possibile elencare una o più operazioni sui file utilizzando un elenco delimitato da virgole. L'elenco per `-file-operations` può includere uno o più dei seguenti valori: • `close` per le operazioni di chiusura del file • `create` per le operazioni di creazione dei file • `create-dir` per le operazioni di creazione directory • `delete` per le operazioni di eliminazione dei file • `delete_dir` per le operazioni di eliminazione della directory • `getattr` per le operazioni get attribute • `link` per le operazioni di collegamento • `lookup` per le operazioni di ricerca • `open` per le operazioni di apertura dei file • `read` per le operazioni di lettura del file • `write` per le operazioni di scrittura del file • `rename` per le operazioni di ridenominazione dei file • `rename_dir` per le operazioni di ridenominazione della directory • `setattr` per le operazioni di set attribute • `symlink` per operazioni di collegamento simbolico Se si specifica `-file-operations`, quindi specificare un protocollo valido in `-protocol` parametro.	`-file-operations file_operations,...`

Filtri Specifica l'elenco dei filtri per una determinata operazione di file per il protocollo specificato. I valori in `-filters` i parametri vengono utilizzati per filtrare le richieste dei client. L'elenco può includere uno o più dei seguenti elementi: Se si specifica `-filters` quindi specificare valori validi per `-file-operations` e. `-protocol` parametri. • `monitor-ads` opzione per filtrare la richiesta del client per un flusso di dati alternativo. • `close-with-modification` opzione per filtrare la richiesta del client per la chiusura con modifica. • `close-without-modification` opzione per filtrare la richiesta del client per la chiusura senza modifiche. • `first-read` opzione per filtrare la richiesta del client per la prima lettura. • `first-write` opzione per filtrare la richiesta del client per la prima scrittura. • `offline-bit` opzione per filtrare la richiesta del client per il set di bit offline. Impostando questo filtro, il server FPolicy riceve una notifica solo quando si accede ai file offline. • `open-with-delete-intent` opzione per filtrare la richiesta del client per l'apertura con intento di eliminazione. Se si imposta questo filtro, il server FPolicy riceve una notifica solo quando si tenta di aprire un file con l'intento di eliminarlo. Questo viene utilizzato dai file system quando `FILE_DELETE_ON_CLOSE` flag specificato. • `open-with-write-intent` opzione per filtrare la richiesta del client per l'apertura con intento di scrittura. L'impostazione di questo filtro comporta la ricezione di una notifica da parte del server FPolicy solo quando si tenta di aprire un file con l'intento di scriverne qualcosa. • `write-with-size-change` opzione per filtrare la richiesta del client per la scrittura con la modifica delle dimensioni. • `setattr-with-owner-change` opzione per filtrare le richieste setattr del client per la modifica del proprietario di un file o di una directory. • `setattr-with-group-change` opzione per filtrare le richieste setattr del client per la modifica del gruppo di un file o di una directory. • `setattr-with-sacl-change` Opzione per filtrare le richieste setattr del client per la modifica del SACL in un file o in una directory. Questo filtro è disponibile solo per i protocolli SMB e NFSv4. • `setattr-with-dacl-change` Opzione per filtrare le richieste setattr	`-filters filter, ...`

È richiesta l'operazione del volume Specifica se il monitoraggio è necessario per le operazioni di montaggio e disinstallazione del volume. L'impostazione predefinita è `false`.	`-volume-operation` {`true`
`false`} `-filters` `filter`, ...	*Notifica accesso FPolicy negata* 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. Le notifiche verranno generate per l'operazione del file non riuscita a causa della mancanza di autorizzazione, che include: • Errori dovuti alle autorizzazioni NTFS. • Errori dovuti a bit di modalità Unix. • Guasti dovuti a ACL NFSv4.
`-monitor-fileop-failure` {`true`	`false`}

Operazioni di file supportate e combinazioni di filtri che FPolicy può monitorare per SMB

Quando si configura l'evento FPolicy, è necessario tenere presente che solo alcune combinazioni di operazioni e filtri dei file sono supportate per il monitoraggio delle operazioni di accesso ai file SMB.

L'elenco delle operazioni di file supportate e delle combinazioni di filtri per il monitoraggio FPolicy degli eventi di accesso ai file SMB è riportato nella seguente tabella:

Operazioni di file supportate	Filtri supportati
chiudere	monitor-ads, offline-bit, close-with-modification, close-without-modification, close-with-read, escludi-directory
creare	monitor-ads, offline-bit

crea_dir	Attualmente non è supportato alcun filtro per questa operazione di file.
eliminare	monitor-ads, offline-bit
dir_delete	Attualmente non è supportato alcun filtro per questa operazione di file.
getattr	offline-bit, exclude-dir
aprire	monitor-ads, offline-bit, open-with-delete-intent, open-with-write-intent, exclude-dir
leggi	monitor-ads, offline-bit, first-read
di scrittura	monitor-ads, offline-bit, first-write, write-with-size-change
rinominare	monitor-ads, offline-bit
rinomina_dir	Attualmente non è supportato alcun filtro per questa operazione di file.
setattr	monitor-ads, offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_creation_time_change, setattr_with_size_change, setattr_with_allocation_size_change, exclude_directory

A partire da ONTAP 9.13.1, gli utenti possono ricevere notifiche per operazioni di file non riuscite a causa della mancanza di autorizzazioni. L'elenco delle combinazioni di filtri e operazioni di accesso negato supportate per il monitoraggio FPolicy degli eventi di accesso ai file SMB è riportato nella seguente tabella:

Operazione di accesso supportato con accesso negato	Filtri supportati
aprire	NA

Operazioni di file supportate e combinazioni di filtri che FPolicy può monitorare per NFSv3

Quando si configura l'evento FPolicy, è necessario tenere presente che solo alcune combinazioni di operazioni e filtri dei file sono supportate per il monitoraggio delle operazioni di accesso ai file NFSv3.

L'elenco delle operazioni di file supportate e delle combinazioni di filtri per il monitoraggio FPolicy degli eventi di accesso al file NFSv3 è riportato nella seguente tabella:

Operazioni di file supportate	Filtri supportati

creare	offline-bit
crea_dir	Attualmente non è supportato alcun filtro per questa operazione di file.
eliminare	offline-bit
dir_delete	Attualmente non è supportato alcun filtro per questa operazione di file.
collegamento	offline-bit
ricerca	offline-bit, exclude-dir
leggi	offline-bit, first-read
di scrittura	offline-bit, first-write, write-with-size-change
rinominare	offline-bit
rinomina_dir	Attualmente non è supportato alcun filtro per questa operazione di file.
setattr	offline-bit, 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
link simbolico	offline-bit

A partire da ONTAP 9.13.1, gli utenti possono ricevere notifiche per operazioni di file non riuscite a causa della mancanza di autorizzazioni. L'elenco delle combinazioni di filtri e operazioni di accesso negato supportate per il monitoraggio FPolicy degli eventi di accesso al file NFSv3 è riportato nella seguente tabella:

Operazione di accesso supportato con accesso negato	Filtri supportati
accesso	NA
creare	NA
crea_dir	NA
eliminare	NA
dir_delete	NA
collegamento	NA

leggi	NA
rinominare	NA
rinomina_dir	NA
setattr	NA
di scrittura	NA

Operazioni di file supportate e combinazioni di filtri che FPolicy può monitorare per NFSv4

Quando si configura l'evento FPolicy, è necessario tenere presente che solo alcune combinazioni di operazioni e filtri dei file sono supportate per il monitoraggio delle operazioni di accesso ai file NFSv4.

A partire da ONTAP 9.15.1, FPolicy supporta il protocollo NFSv4,1.

L'elenco delle combinazioni di operazioni e filtri supportate per il monitoraggio FPolicy degli eventi di accesso ai file NFSv4 o NFSv4,1 è fornito nella tabella seguente:

Operazioni di file supportate	Filtri supportati
chiudere	offline-bit, exclude-directory
creare	offline-bit
crea_dir	Attualmente non è supportato alcun filtro per questa operazione di file.
eliminare	offline-bit
dir_delete	Attualmente non è supportato alcun filtro per questa operazione di file.
getattr	offline-bit, exclude-directory
collegamento	offline-bit
ricerca	offline-bit, exclude-directory
aprire	offline-bit, exclude-directory
leggi	offline-bit, first-read
di scrittura	offline-bit, first-write, write-with-size-change

rinominare	offline-bit
rinomina_dir	Attualmente non è supportato alcun filtro per questa operazione di file.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
link simbolico	offline-bit

A partire da ONTAP 9.13.1, gli utenti possono ricevere notifiche per operazioni di file non riuscite a causa della mancanza di autorizzazioni. L'elenco delle combinazioni di filtri e delle operazioni sui file con accesso negato supportate per il monitoraggio FPolicy degli eventi di accesso ai file NFSv4 o NFSv4,1 è riportato nella tabella seguente:

Operazione di accesso supportato con accesso negato	Filtri supportati
accesso	NA
creare	NA
crea_dir	NA
eliminare	NA
dir_delete	NA
collegamento	NA
aprire	NA
leggi	NA
rinominare	NA
rinomina_dir	NA
setattr	NA
di scrittura	NA

Completare il foglio di lavoro di configurazione degli eventi FPolicy

È possibile utilizzare questo foglio di lavoro per registrare i valori necessari durante il processo di configurazione degli eventi FPolicy. Se è richiesto un valore di parametro, è necessario determinare quale valore utilizzare per tali parametri prima di configurare l'evento FPolicy.

Registrare se si desidera includere ogni impostazione di parametro nella configurazione dell'evento FPolicy e quindi registrare il valore dei parametri che si desidera includere.

Tipo di informazione	Obbligatorio	Includi	I tuoi valori
Nome SVM (Storage Virtual Machine)	Sì	Sì	
Nome dell'evento	Sì	Sì	
Protocollo	No		
Operazioni sui file	No		
Filtri	No		
Funzionamento del volume	No		
Accesso agli eventi negati + (supporto a partire da ONTAP 9.13)	No		

Pianificare la configurazione del criterio FPolicy

Pianificare la panoramica della configurazione dei criteri FPolicy

Prima di configurare il criterio FPolicy, è necessario comprendere quali parametri sono necessari per la creazione del criterio e perché si desidera configurare determinati parametri opzionali. Queste informazioni consentono di determinare i valori da impostare per ciascun parametro.

Quando si crea un criterio FPolicy, si associa il criterio a quanto segue:

- La macchina virtuale per lo storage (SVM)
- Uno o più eventi FPolicy
- Un motore esterno FPolicy

È inoltre possibile configurare diverse impostazioni opzionali dei criteri.

Contenuto della configurazione del criterio FPolicy

Per pianificare la configurazione, è possibile utilizzare il seguente elenco di criteri FPolicy obbligatori e parametri opzionali:

Tipo di informazione	Opzione	Obbligatorio	Predefinito
Nome SVM Specifica il nome della SVM su cui si desidera creare un criterio FPolicy.	`-vserver vserver_name`	Sì	Nessuno
Nome policy Specifica il nome del criterio FPolicy. Il nome può contenere fino a 256 caratteri. Se si configura il criterio in una configurazione di disaster recovery MetroCluster o SVM, il nome deve contenere fino a 200 caratteri. Il nome può contenere qualsiasi combinazione dei seguenti caratteri ASCII: • `a` attraverso `z` • `A` attraverso `Z` • `0` attraverso `9` • “_”, “-”, and "``"	`-policy-name policy_name`	Sì	Nessuno
Nomi eventi Specifica un elenco delimitato da virgole di eventi da associare al criterio FPolicy. • È possibile associare più di un evento a un criterio. • Un evento è specifico di un protocollo. • È possibile utilizzare un singolo criterio per monitorare gli eventi di accesso ai file per più protocolli creando un evento per ciascun protocollo che si desidera monitorare dal criterio e associando quindi gli eventi al criterio. • Gli eventi devono già esistere.	`-events event_name, ...`	Sì	Nessuno

Archivio persistente A partire da ONTAP 9.14.1, questo parametro specifica l'archivio persistente per acquisire eventi di accesso ai file per le policy asincrone non obbligatorie nella SVM.	`-persistent -store persistent_store_name`	No	Nessuno
Nome motore esterno Specifica il nome del motore esterno da associare al criterio FPolicy. • Un motore esterno contiene le informazioni richieste dal nodo per inviare le notifiche a un server FPolicy. • È possibile configurare FPolicy per utilizzare il motore esterno nativo di ONTAP per un semplice blocco dei file o per utilizzare un motore esterno configurato per utilizzare server FPolicy esterni (server FPolicy) per un blocco dei file e una gestione dei file più sofisticati. • Se si desidera utilizzare il motore esterno nativo, non è possibile specificare un valore per questo parametro o è possibile specificare `native` come valore. • Se si desidera utilizzare i server FPolicy, la configurazione per il motore esterno deve già esistere.	`-engine engine_name`	Sì (a meno che il criterio non utilizzi il motore nativo ONTAP interno)	`native`
È richiesto lo screening obbligatorio Specifica se è richiesto lo screening obbligatorio dell'accesso ai file. • L'impostazione di screening obbligatorio determina l'azione intrapresa in caso di evento di accesso al file in caso di inattività di tutti i server primari e secondari o di mancata ricezione di una risposta dai server FPolicy entro un determinato periodo di timeout. • Quando è impostato su `true`, gli eventi di accesso al file sono negati. • Quando è impostato su `false`, sono consentiti eventi di accesso al file.	`-is-mandatory` {`true`	`false`}	No

`true`	*Consenti accesso privilegiato* Specifica se si desidera che il server FPolicy disponga di un accesso privilegiato ai file e alle cartelle monitorati utilizzando una connessione dati con privilegi. Se configurati, i server FPolicy possono accedere ai file dalla directory principale della SVM contenente i dati monitorati utilizzando la connessione dati con privilegi. Per un accesso privilegiato ai dati, SMB deve essere concesso in licenza sul cluster e tutti i dati LIF utilizzati per connettersi ai server FPolicy devono essere configurati in modo da avere `cifs` come uno dei protocolli consentiti. Se si desidera configurare il criterio per consentire l'accesso con privilegi, è necessario specificare anche il nome utente dell'account che il server FPolicy deve utilizzare per l'accesso con privilegi.	`-allow -privileged -access` {`yes`	`no`}

No (a meno che non sia attivata la funzione pass-through-Read)	`no`	*Nome utente privilegiato* Specifica il nome utente dell'account utilizzato dai server FPolicy per l'accesso ai dati con privilegi. • Il valore di questo parametro deve utilizzare il formato "`domain` user name". • Se `-allow -privileged -access` è impostato su `no`, qualsiasi valore impostato per questo parametro viene ignorato.	`-privileged -user-name user_name`

No (a meno che non sia abilitato l'accesso privilegiato)	Nessuno	*Allow pass-through-Read* Specifica se i server FPolicy possono fornire servizi di lettura pass-through per i file che sono stati archiviati nello storage secondario (file offline) dai server FPolicy: • La lettura pass-through è un modo per leggere i dati per i file offline senza ripristinarli nello storage primario. La funzione Passthrough-Read riduce le latenze delle risposte, poiché non è necessario richiamare i file sullo storage primario prima di rispondere alla richiesta di lettura. Inoltre, la funzione pass-through-Read ottimizza l'efficienza dello storage eliminando la necessità di consumare spazio di storage primario con file richiamati esclusivamente per soddisfare le richieste di lettura. • Se attivati, i server FPolicy forniscono i dati per il file su un canale dati privilegiato	`-is-passthrough-read-enabled {true`

Requisito per le configurazioni dell'ambito FPolicy se il criterio FPolicy utilizza il motore nativo

Se si configura il criterio FPolicy per utilizzare il motore nativo, esiste un requisito specifico per la definizione dell'ambito FPolicy configurato per il criterio.

L'ambito FPolicy definisce i limiti ai quali si applica il criterio FPolicy, ad esempio se FPolicy si applica a volumi o condivisioni specificati. Esistono diversi parametri che limitano ulteriormente l'ambito a cui si applica la policy FPolicy. Uno di questi parametri, `-is-file-extension-check-on-directories-enabled`, specifica se controllare le estensioni dei file nelle directory. Il valore predefinito è `false`, che significa che le estensioni dei file nelle directory non sono selezionate.

Quando un criterio FPolicy che utilizza il motore nativo è attivato su una condivisione o volume e su `-is-file-extension-check-on-directories-enabled` il parametro è impostato su `false` per l'ambito del criterio, l'accesso alla directory viene negato. Con questa configurazione, poiché le estensioni dei file non vengono controllate per le directory, qualsiasi operazione di directory viene negata se rientra nell'ambito del criterio.

Per garantire che l'accesso alla directory abbia esito positivo quando si utilizza il motore nativo, è necessario impostare `-is-file-extension-check-on-directories-enabled parameter` a. `true` quando si crea l'ambito.

Con questo parametro impostato su `true`, I controlli delle estensioni vengono eseguiti per le operazioni di directory e la decisione di consentire o negare l'accesso viene presa in base alle estensioni incluse o escluse nella configurazione dell'ambito FPolicy.

Completare il foglio di lavoro della policy FPolicy

È possibile utilizzare questo foglio di lavoro per registrare i valori necessari durante il processo di configurazione dei criteri FPolicy. Registrare se si desidera includere ciascuna impostazione di parametro nella configurazione del criterio FPolicy e quindi registrare il valore dei parametri che si desidera includere.

Tipo di informazione	Includi	I tuoi valori
Nome SVM (Storage Virtual Machine)	Sì	
Nome policy	Sì	
Nomi degli eventi	Sì	
Archivio persistente		
Nome del motore esterno		
È richiesto lo screening obbligatorio?		
Consentire l'accesso con privilegi		

Nome utente con privilegi		
Il pass-through-Read è abilitato?		

Pianificare la configurazione dell’ambito FPolicy

Pianificare la panoramica della configurazione dell’ambito FPolicy

Prima di configurare l’ambito di FPolicy, è necessario comprendere il significato di creazione di un ambito. È necessario comprendere cosa contiene la configurazione dell’ambito. È inoltre necessario comprendere quali sono le regole di priorità dell’ambito. Queste informazioni consentono di pianificare i valori che si desidera impostare.

Cosa significa creare un ambito FPolicy

La creazione dell’ambito FPolicy significa definire i limiti ai quali si applica il criterio FPolicy. La macchina virtuale per lo storage (SVM) è il limite di base. Quando si crea un ambito per un criterio FPolicy, è necessario definire il criterio FPolicy a cui si applicherà ed è necessario indicare a quale SVM si desidera applicare l’ambito.

Esistono diversi parametri che limitano ulteriormente l’ambito all’interno della SVM specificata. È possibile limitare l’ambito specificando cosa includere nell’ambito o cosa escludere dall’ambito. Dopo aver applicato un ambito a un criterio abilitato, i controlli degli eventi del criterio vengono applicati all’ambito definito da questo comando.

Le notifiche vengono generate per gli eventi di accesso ai file in cui le corrispondenze si trovano nelle opzioni “include”. Le notifiche non vengono generate per gli eventi di accesso al file in cui sono presenti corrispondenze nelle opzioni “exclude”.

La configurazione dell’ambito FPolicy definisce le seguenti informazioni di configurazione:

- Nome SVM
- Nome policy
- Le condivisioni da includere o escludere da ciò che viene monitorato
- Le policy di esportazione da includere o escludere da ciò che viene monitorato
- I volumi da includere o escludere da ciò che viene monitorato
- Le estensioni di file da includere o escludere da ciò che viene monitorato
- Se eseguire il controllo dell’estensione del file sugli oggetti di directory

> Esistono considerazioni particolari per l'ambito di applicazione di una policy FPolicy del cluster. Il criterio FPolicy del cluster è un criterio creato dall'amministratore del cluster per la SVM amministrativa. Se l'amministratore del cluster crea anche l'ambito per il criterio FPolicy del cluster, l'amministratore SVM non può creare un ambito per lo stesso criterio. Tuttavia, se l'amministratore del cluster non crea un ambito per il criterio FPolicy del cluster, qualsiasi amministratore SVM può creare l'ambito per tale criterio del cluster. Se l'amministratore di SVM crea un ambito per tale criterio FPolicy del cluster, l'amministratore del cluster non potrà successivamente creare un ambito del cluster per lo stesso criterio del cluster. Questo perché l'amministratore del cluster non può eseguire l'override dell'ambito per lo stesso criterio del cluster.

Quali sono le regole di priorità dell'ambito di applicazione

Le seguenti regole di precedenza si applicano alle configurazioni dell'ambito:

- Quando una condivisione è inclusa in `-shares-to-include` il parametro e il volume padre della condivisione sono inclusi in `-volumes-to-exclude` parametro, `-volumes-to-exclude` ha la precedenza `-shares-to-include`.
- Quando un criterio di esportazione viene incluso in `-export-policies-to-include` il parametro e il volume principale del criterio di esportazione sono inclusi in `-volumes-to-exclude` parametro, `-volumes-to-exclude` ha la precedenza `-export-policies-to-include`.
- Un amministratore può specificare entrambi `-file-extensions-to-include` e. `-file-extensions -to-exclude` elenchi.

  Il `-file-extensions-to-exclude` il parametro viene controllato prima di `-file-extensions-to -include` parametro selezionato.

Contenuto della configurazione FPolicy Scope

È possibile utilizzare il seguente elenco di parametri di configurazione FPolicy Scope disponibili per pianificare la configurazione:

> Quando si configurano le condivisioni, le policy di esportazione, i volumi e le estensioni dei file da includere o escludere dall'ambito, i parametri include ed exclude possono includere metacaratteri come "?" and "*". L'utilizzo delle espressioni regolari non è supportato.

Tipo di informazione	Opzione
SVM Specifica il nome SVM su cui si desidera creare un ambito FPolicy. Ogni configurazione FPolicy viene definita all'interno di una singola SVM. Il motore esterno, l'evento del criterio, l'ambito del criterio e il criterio che si combinano insieme per creare una configurazione del criterio FPolicy devono essere tutti associati alla stessa SVM.	`-vserver vserver_name`

Nome policy Specifica il nome del criterio FPolicy a cui si desidera associare l'ambito. Il criterio FPolicy deve già esistere.	`-policy-name policy_name`
Condivisioni da includere Specifica un elenco delimitato da virgole di condivisioni da monitorare per il criterio FPolicy a cui viene applicato l'ambito.	`-shares-to-include share_name, ...`
Condivisioni da escludere Specifica un elenco delimitato da virgole di condivisioni da escludere dal monitoraggio per il criterio FPolicy a cui viene applicato l'ambito.	`-shares-to-exclude share_name, ...`
Volumi da includere specifica un elenco di volumi delimitati da virgole da monitorare per il criterio FPolicy a cui viene applicato l'ambito.	`-volumes-to-include volume_name, ...`
Volumi da escludere Specifica un elenco delimitato da virgole di volumi da escludere dal monitoraggio per il criterio FPolicy a cui viene applicato l'ambito.	`-volumes-to-exclude volume_name, ...`
Esporta policy da includere Specifica un elenco delimitato da virgole di criteri di esportazione da monitorare per il criterio FPolicy a cui viene applicato l'ambito.	`-export-policies-to -include export_policy_name, ...`
Esporta policy da escludere Specifica un elenco delimitato da virgole di criteri di esportazione da escludere dal monitoraggio per il criterio FPolicy a cui viene applicato l'ambito.	`-export-policies-to -exclude export_policy_name, ...`
Estensioni file da includere Specifica un elenco delimitato da virgole di estensioni di file da monitorare per il criterio FPolicy a cui viene applicato l'ambito.	`-file-extensions-to -include file_extensions, ...`
Estensione del file da escludere Specifica un elenco delimitato da virgole di estensioni di file da escludere dal monitoraggio del criterio FPolicy a cui viene applicato l'ambito.	`-file-extensions-to -exclude file_extensions, ...`

Il controllo dell'estensione del file sulla directory è abilitato ? Specifica se i controlli dell'estensione del nome file si applicano anche agli oggetti di directory. Se questo parametro è impostato su `true`, gli oggetti di directory sono sottoposti agli stessi controlli di estensione dei file normali. Se questo parametro è impostato su `false`, i nomi delle directory non corrispondono per gli interni e le notifiche vengono inviate per le directory anche se le relative estensioni non corrispondono. Se il criterio FPolicy a cui è assegnato l'ambito è configurato per utilizzare il motore nativo, questo parametro deve essere impostato su `true`.	`-is-file-extension -check-on-directories -enabled` {`true`
`false`	}

Completare il foglio di lavoro FPolicy Scope

È possibile utilizzare questo foglio di lavoro per registrare i valori necessari durante il processo di configurazione dell'ambito FPolicy. Se è richiesto un valore di parametro, è necessario determinare quale valore utilizzare per tali parametri prima di configurare l'ambito FPolicy.

Registrare se si desidera includere ciascuna impostazione di parametro nella configurazione dell'ambito FPolicy e quindi registrare il valore dei parametri che si desidera includere.

Tipo di informazione	Obbligatorio	Includi	I tuoi valori
Nome SVM (Storage Virtual Machine)	Sì	Sì	
Nome policy	Sì	Sì	
Condivisioni da includere	No		
Condivisioni da escludere	No		
Volumi da includere	No		
Volumi da escludere	No		
Policy di esportazione da includere	No		
Esportare i criteri da escludere	No		
Estensioni di file da includere	No		
Estensione del file da escludere	No		

Il controllo dell’estensione del file nella directory è attivato?	No		