Utilizzare FPolicy per il monitoraggio e la gestione dei file su SVM

ONTAP 9

NetApp
April 24, 2024

Sommario

Utilizzare FPolicy per il monitoraggio e la gestione dei file su SVM

Comprendere FPolicy

Quali sono le due parti della soluzione FPolicy

FPolicy è un framework di notifica dell'accesso ai file utilizzato per monitorare e gestire gli eventi di accesso ai file sulle macchine virtuali di storage (SVM) attraverso le soluzioni dei partner. Le soluzioni dei partner ti aiutano a risolvere diversi casi di utilizzo, ad esempio governance e conformità dei dati, protezione ransomware e mobilità dei dati.

Le soluzioni dei partner includono soluzioni di terze parti supportate da NetApp e prodotti NetApp per la sicurezza del carico di lavoro e il rilevamento dei dati nel cloud.

Una soluzione FPolicy è composta da due parti. Il framework FPolicy di ONTAP gestisce le attività sul cluster e invia notifiche all'applicazione partner (alias server FPolicy esterni). I server FPolicy esterni elaborano le notifiche inviate da ONTAP FPolicy per soddisfare i casi di utilizzo dei clienti.

Il framework ONTAP crea e gestisce la configurazione di FPolicy, monitora gli eventi dei file e invia notifiche ai server FPolicy esterni. ONTAP FPolicy fornisce l'infrastruttura che consente la comunicazione tra server FPolicy esterni e nodi SVM (Storage Virtual Machine).

Il framework FPolicy si connette ai server FPolicy esterni e invia notifiche per determinati eventi del file system ai server FPolicy quando questi eventi si verificano in seguito all'accesso del client. I server FPolicy esterni elaborano le notifiche e inviano le risposte al nodo. Ciò che accade in seguito all'elaborazione delle notifiche dipende dall'applicazione e dal fatto che la comunicazione tra il nodo e i server esterni sia asincrona o sincrona.

Quali sono le notifiche sincrone e asincrone

FPolicy invia notifiche ai server FPolicy esterni tramite l'interfaccia FPolicy. Le notifiche vengono inviate in modalità sincrona o asincrona. La modalità di notifica determina le operazioni di ONTAP dopo l'invio di notifiche ai server FPolicy.

- **Notifiche asincrone**

  Con le notifiche asincrone, il nodo non attende una risposta dal server FPolicy, che migliora il throughput complessivo del sistema. Questo tipo di notifica è adatto alle applicazioni in cui il server FPolicy non richiede che venga intrapresa alcuna azione in seguito alla valutazione della notifica. Ad esempio, le notifiche asincrone vengono utilizzate quando l'amministratore della macchina virtuale di storage (SVM) desidera monitorare e controllare l'attività di accesso ai file.

  Se un server FPolicy che opera in modalità asincrona subisce un'interruzione di rete, le notifiche FPolicy generate durante l'interruzione vengono memorizzate nel nodo di storage. Quando il server FPolicy torna in linea, viene avvisato delle notifiche memorizzate e può recuperarle dal nodo di storage. Il periodo di tempo in cui le notifiche possono essere memorizzate durante un'interruzione è configurabile fino a 10 minuti.

  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.

- **Notifiche sincrona**

  Se configurato per l'esecuzione in modalità sincrona, il server FPolicy deve riconoscere ogni notifica prima che l'operazione del client possa continuare. Questo tipo di notifica viene utilizzato quando è richiesta un'azione in base ai risultati della valutazione della notifica. Ad esempio, le notifiche sincrone vengono utilizzate quando l'amministratore SVM desidera consentire o negare le richieste in base ai criteri specificati sul server FPolicy esterno.

Applicazioni sincrone e asincrone

Esistono molti possibili utilizzi per le applicazioni FPolicy, sia asincrone che sincrona.

Le applicazioni asincrone sono quelle in cui il server FPolicy esterno non altera l'accesso a file o directory o non modifica i dati sulla macchina virtuale di storage (SVM). Ad esempio:

- Accesso al file e registrazione dell'audit
- Gestione delle risorse dello storage

Le applicazioni sincrone sono quelle in cui l'accesso ai dati viene alterato o i dati vengono modificati dal server FPolicy esterno. Ad esempio:

- Gestione delle quote
- Blocco dell'accesso al file
- Archiviazione dei file e gestione dello storage gerarchico
- Servizi di crittografia e decrittografia
- Servizi di compressione e decompressione

Archivi persistenti di FPolicy

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.

Questa funzione è disponibile solo in modalità FPolicy esterna. L'applicazione partner utilizzata deve supportare questa funzione. È necessario collaborare con il proprio partner per assicurarsi che questa configurazione FPolicy sia supportata.

Best practice

Gli amministratori del cluster devono configurare un volume per l'archivio persistente in ciascuna SVM dove FPolicy è abilitato. Una volta configurato, un archivio persistente acquisisce tutti gli eventi FPolicy corrispondenti, che vengono ulteriormente elaborati nella pipeline FPolicy e inviati al server esterno.

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 verranno 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 sono ancora state elaborate verranno spostate anche nel nuovo nodo. Sarà necessario eseguire nuovamente `fpolicy persistent-store create` su uno dei nodi dopo lo spostamento del volume, per garantire che la notifica in sospeso venga inviata al server esterno.

Il volume dello storage persistente viene configurato in base alle singole SVM. Per ogni SVM abilitata per FPolicy dovrai creare un volume archivio persistente.

Crea il volume di archivio persistente sul nodo con LIF che prevedono il monitoraggio del traffico massimo da parte di 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.

Il nome del volume di archiviazione persistente e il percorso di giunzione specificati al momento della creazione del volume dovrebbero corrispondere.

Impostare il criterio snapshot su `none` per quel volume 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.

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. Per ottenere questo risultato, dopo aver attivato FPolicy, smontare il volume in ONTAP per rimuovere il percorso di giunzione; ciò lo rende inaccessibile per l'accesso al protocollo utente.

Per ulteriori informazioni, vedere "Creare archivi persistenti".

Tipi di configurazione FPolicy

Esistono due tipi di configurazione FPolicy di base. Una configurazione utilizza server FPolicy esterni per elaborare e agire in base alle notifiche. L'altra configurazione non utilizza server FPolicy esterni, ma utilizza il server FPolicy nativo interno di ONTAP per un semplice blocco dei file basato sulle estensioni.

- **Configurazione del server FPolicy esterno**

  La notifica viene inviata al server FPolicy, che vagli la richiesta e applica le regole per determinare se il nodo deve consentire l'operazione di file richiesta. Per i criteri sincroni, il server FPolicy invia quindi una risposta al nodo per consentire o bloccare l'operazione di file richiesta.

- **Configurazione del server FPolicy nativo**

  La notifica viene sottoposta a screening interno. La richiesta viene consentita o negata in base alle impostazioni di estensione del file configurate nell'ambito FPolicy.

  Nota: Le richieste di estensione del file negate non vengono registrate.

Quando creare una configurazione FPolicy nativa

Le configurazioni FPolicy native utilizzano il motore FPolicy interno di ONTAP per monitorare e bloccare le operazioni dei file in base all'estensione del file. Questa soluzione non richiede server FPolicy esterni (server FPolicy). L'utilizzo di una configurazione nativa per il blocco dei file è appropriato quando questa semplice soluzione è tutto ciò che serve.

Il blocco nativo dei file consente di monitorare le operazioni dei file che corrispondono alle operazioni configurate e agli eventi di filtraggio, negando quindi l'accesso ai file con estensioni particolari. Questa è la configurazione predefinita.

Questa configurazione consente di bloccare l'accesso al file solo in base all'estensione del file. Ad esempio, per bloccare i file che contengono `mp3` extensions (estensioni), viene configurato un criterio per fornire notifiche per determinate operazioni con estensioni file di destinazione di `mp3`. Il criterio è configurato per negare `mp3` richieste di file per operazioni che generano notifiche.

Quanto segue si applica alle configurazioni FPolicy native:

- Lo stesso set di filtri e protocolli supportati dallo screening dei file basato su server FPolicy è supportato anche per il blocco dei file nativi.
- È possibile configurare contemporaneamente le applicazioni di blocco dei file nativi e di screening dei file basate su server FPolicy.

  A tale scopo, è possibile configurare due policy FPolicy separate per la macchina virtuale di storage (SVM), una configurata per il blocco dei file nativi e una configurata per lo screening dei file basato su server FPolicy.

- La funzione di blocco dei file nativi consente di visualizzare solo i file in base alle estensioni e non in base al contenuto del file.
- Nel caso di collegamenti simbolici, il blocco dei file nativi utilizza l'estensione del file root.

Scopri di più "FPolicy: Blocco dei file nativi".

Quando creare una configurazione che utilizza server FPolicy esterni

Le configurazioni FPolicy che utilizzano server FPolicy esterni per elaborare e gestire le notifiche offrono soluzioni efficaci per i casi di utilizzo in cui è necessario un blocco dei file più semplice basato sull'estensione dei file.

È necessario creare una configurazione che utilizzi server FPolicy esterni quando si desidera eseguire operazioni quali il monitoraggio e la registrazione degli eventi di accesso ai file, fornire servizi di quota, eseguire il blocco dei file in base a criteri diversi dalle semplici estensioni dei file, fornire servizi di migrazione dei dati utilizzando applicazioni di gestione dello storage gerarchiche, In alternativa, è possibile fornire un insieme di policy dettagliato che monitorano solo un sottoinsieme di dati nella macchina virtuale di storage (SVM).

Ruoli che i componenti del cluster giocano con l'implementazione di FPolicy

Il cluster, le SVM (Storage Virtual Machine) contenute e le LIF dei dati svolgono un ruolo fondamentale in un'implementazione FPolicy.

- **cluster**

  Il cluster contiene il framework di gestione FPolicy e gestisce e gestisce le informazioni su tutte le

configurazioni FPolicy nel cluster.

- **SVM**

  Viene definita una configurazione FPolicy a livello di SVM. L'ambito della configurazione è SVM e funziona solo con le risorse SVM. Una configurazione SVM non è in grado di monitorare e inviare notifiche per le richieste di accesso ai file effettuate per i dati che risiedono su un'altra SVM.

  Le configurazioni FPolicy possono essere definite sulla SVM amministrativa. Una volta definite le configurazioni sulla SVM amministrativa, queste possono essere visualizzate e utilizzate in tutte le SVM.

- **LIF dati**

  Le connessioni ai server FPolicy vengono effettuate tramite i LIF dei dati appartenenti a SVM con la configurazione FPolicy. I dati LIF utilizzati per queste connessioni possono eseguire il failover nello stesso modo dei dati LIF utilizzati per il normale accesso client.

Funzionamento di FPolicy con i server FPolicy esterni

Dopo aver configurato e attivato FPolicy sulla macchina virtuale di storage (SVM), FPolicy viene eseguito su ogni nodo a cui partecipa SVM. FPolicy è responsabile della creazione e della gestione delle connessioni con server FPolicy esterni (server FPolicy), dell'elaborazione delle notifiche e della gestione dei messaggi di notifica da e verso i server FPolicy.

Inoltre, nell'ambito della gestione delle connessioni, FPolicy ha le seguenti responsabilità:

- Garantisce che la notifica del file scorra attraverso la LIF corretta al server FPolicy.
- Garantisce che quando più server FPolicy sono associati a un criterio, il bilanciamento del carico viene eseguito quando si inviano notifiche ai server FPolicy.
- Tenta di ristabilire la connessione in caso di interruzione della connessione a un server FPolicy.
- Invia le notifiche ai server FPolicy in una sessione autenticata.
- Gestisce la connessione dati pass-through-Read stabilita dal server FPolicy per gestire le richieste del client quando è attivata la funzione pass-through-Read.

Come vengono utilizzati i canali di controllo per la comunicazione FPolicy

FPolicy avvia una connessione del canale di controllo a un server FPolicy esterno dalle LIF dei dati di ciascun nodo che partecipa a una macchina virtuale di storage (SVM). FPolicy utilizza canali di controllo per la trasmissione delle notifiche dei file; pertanto, un server FPolicy potrebbe visualizzare più connessioni dei canali di controllo in base alla topologia SVM.

Come vengono utilizzati i canali di accesso privilegiato ai dati per le comunicazioni sincrone

Con i casi di utilizzo sincroni, il server FPolicy accede ai dati che risiedono sulla macchina virtuale di storage (SVM) attraverso un percorso di accesso privilegiato ai dati. L'accesso attraverso il percorso privilegiato espone l'intero file system al server FPolicy. Il reparto IT può accedere ai file di dati per raccogliere informazioni, scansionare file, leggere file o scrivere in file.

Poiché il server FPolicy esterno può accedere all'intero file system dalla directory principale di SVM attraverso il canale dati privilegiato, la connessione del canale dati privilegiato deve essere sicura.

Modalità di utilizzo delle credenziali di connessione FPolicy con i canali di accesso privilegiato ai dati

Il server FPolicy effettua connessioni privilegiate di accesso ai dati ai nodi del cluster utilizzando una specifica credenziale utente Windows che viene salvata con la configurazione FPolicy. SMB è l'unico protocollo supportato per la connessione di un canale di accesso privilegiato ai dati.

Se il server FPolicy richiede un accesso privilegiato ai dati, devono essere soddisfatte le seguenti condizioni:

- Sul cluster deve essere attivata una licenza SMB.
- Il server FPolicy deve essere eseguito con le credenziali configurate nella configurazione FPolicy.

Quando si effettua una connessione al canale dati, FPolicy utilizza la credenziale per il nome utente Windows specificato. L'accesso ai dati avviene tramite la condivisione amministrativa ONTAP_ADMIN.

Cosa significa concedere credenziali super utente per l'accesso privilegiato ai dati

ONTAP utilizza la combinazione dell'indirizzo IP e della credenziale utente configurata nella configurazione FPolicy per assegnare credenziali super utente al server FPolicy.

Quando il server FPolicy accede ai dati, lo stato di Super User concede i seguenti privilegi:

- Evitare controlli delle autorizzazioni

  L'utente evita di controllare i file e l'accesso alla directory.

- Speciali privilegi di blocco

  ONTAP consente l'accesso in lettura, scrittura o modifica a qualsiasi file, indipendentemente dai blocchi esistenti. Se il server FPolicy utilizza blocchi di intervallo di byte sul file, si ottiene la rimozione immediata dei blocchi esistenti sul file.

- Ignorare eventuali controlli FPolicy

  Access non genera alcuna notifica FPolicy.

In che modo FPolicy gestisce l'elaborazione delle policy

Alla macchina virtuale di storage (SVM) potrebbero essere assegnati più criteri FPolicy, ciascuno con una priorità diversa. Per creare una configurazione FPolicy appropriata sulla SVM, è importante comprendere come FPolicy gestisce l'elaborazione delle policy.

Ogni richiesta di accesso al file viene inizialmente valutata per determinare quali policy monitorano questo evento. Se si tratta di un evento monitorato, le informazioni sull'evento monitorato e le policy interessate vengono trasmesse a FPolicy, dove vengono valutate. Ogni policy viene valutata in base alla priorità assegnata.

Durante la configurazione dei criteri, è necessario prendere in considerazione i seguenti consigli:

- Se si desidera che un criterio venga sempre valutato prima di altri criteri, configurarlo con una priorità più alta.
- Se il successo dell'operazione di accesso al file richiesta in un evento monitorato è un prerequisito per una richiesta di file che viene valutata in base a un altro criterio, assegnare una priorità maggiore alla policy che controlla il successo o l'errore della prima operazione di file.

Ad esempio, se un criterio gestisce la funzionalità di archiviazione e ripristino dei file FPolicy e un secondo criterio gestisce le operazioni di accesso ai file sul file online, il criterio che gestisce il ripristino dei file deve avere una priorità più alta in modo che il file venga ripristinato prima di poter consentire l'operazione gestita dal secondo criterio.

- Se si desidera valutare tutti i criteri applicabili a un'operazione di accesso ai file, assegnare una priorità inferiore ai criteri sincroni.

È possibile riordinare le priorità dei criteri per i criteri esistenti modificando il numero di sequenza dei criteri. Tuttavia, per fare in modo che FPolicy valuti i criteri in base all'ordine di priorità modificato, è necessario disattivare e riabilitare il criterio con il numero di sequenza modificato.

Qual è il processo di comunicazione da nodo a server FPolicy esterno

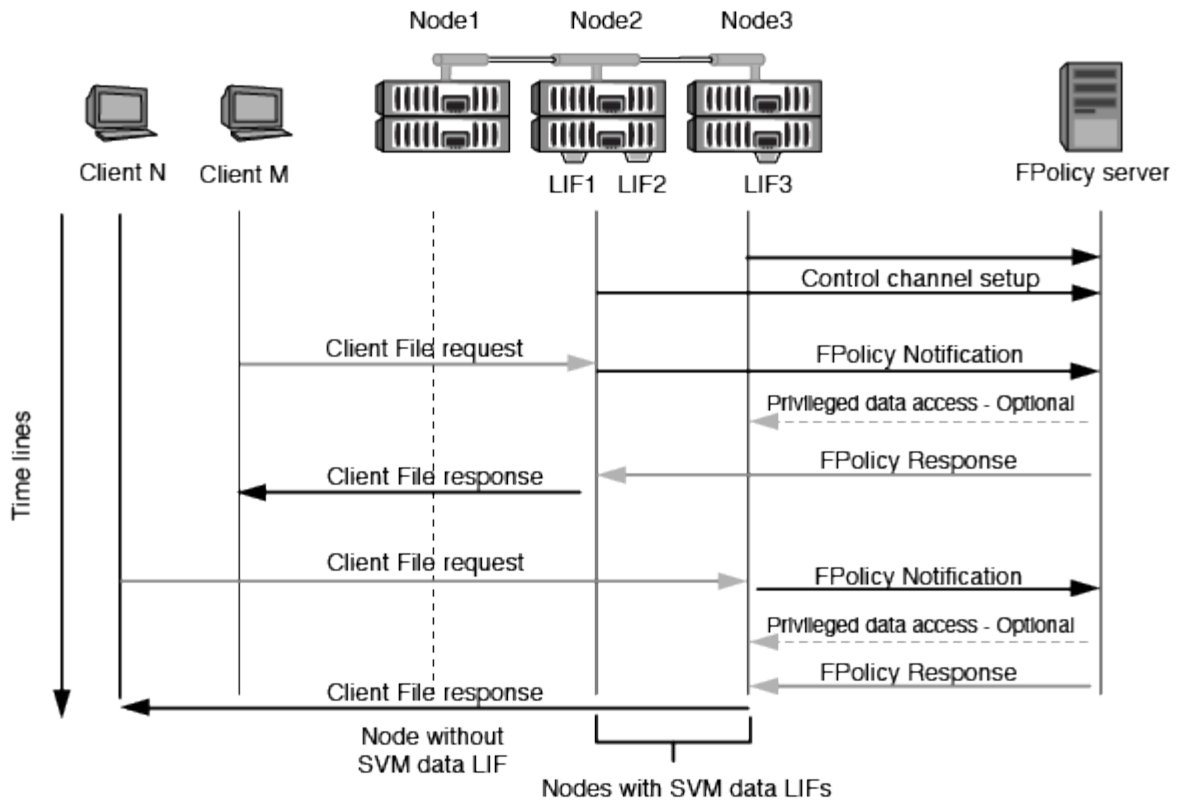
Per pianificare correttamente la configurazione di FPolicy, è necessario comprendere il processo di comunicazione da nodo a server FPolicy esterno.

Ogni nodo che partecipa a ciascuna macchina virtuale di storage (SVM) avvia una connessione a un server FPolicy esterno (server FPolicy) utilizzando TCP/IP. Le connessioni ai server FPolicy vengono configurate utilizzando LIF dei dati dei nodi; pertanto, un nodo partecipante può impostare una connessione solo se il nodo dispone di una LIF dei dati operativi per SVM.

Ogni processo FPolicy sui nodi partecipanti tenta di stabilire una connessione con il server FPolicy quando il criterio è attivato. Utilizza l'indirizzo IP e la porta del motore esterno FPolicy specificato nella configurazione del criterio.

La connessione stabilisce un canale di controllo da ciascuno dei nodi che partecipano a ciascuna SVM al server FPolicy attraverso la LIF dei dati. Inoltre, se gli indirizzi LIF dei dati IPv4 e IPv6 sono presenti sullo stesso nodo partecipante, FPolicy tenta di stabilire connessioni sia per IPv4 che per IPv6. Pertanto, in uno scenario in cui la SVM si estende su più nodi o se sono presenti entrambi gli indirizzi IPv4 e IPv6, il server FPolicy deve essere pronto per più richieste di configurazione del canale di controllo dal cluster dopo che la policy FPolicy è stata attivata sulla SVM.

Ad esempio, se un cluster ha tre nodi - Node1, Node2 e node3 - e le LIF dei dati SVM sono distribuite solo su Node2 e node3, i canali di controllo vengono avviati solo da Node2 e node3, indipendentemente dalla distribuzione dei volumi di dati. Si supponga che Node2 abbia due LIF di dati (LIF e LF2) che appartengono alla SVM e che la connessione iniziale sia da LIF. In caso di errore di LIF, FPolicy tenta di stabilire un canale di controllo da LIE2.



Come FPolicy gestisce le comunicazioni esterne durante la migrazione LIF o il failover

È possibile migrare le LIF dei dati nelle porte dati dello stesso nodo o nelle porte dati di un nodo remoto.

Quando si esegue il failover o la migrazione di una LIF dati, viene stabilita una nuova connessione del canale di controllo al server FPolicy. FPolicy può quindi riprovare le richieste dei client SMB e NFS in timeout, con il risultato che le nuove notifiche vengono inviate ai server FPolicy esterni. Il nodo rifiuta le risposte del server FPolicy alle richieste SMB e NFS originali, con timeout.

Come FPolicy gestisce le comunicazioni esterne durante il failover del nodo

Se il nodo del cluster che ospita le porte dati utilizzate per la comunicazione FPolicy non riesce, ONTAP interrompe la connessione tra il server FPolicy e il nodo.

L'impatto del failover del cluster sul server FPolicy può essere mitigato configurando il criterio di failover per migrare la porta dati utilizzata nella comunicazione FPolicy a un altro nodo attivo. Una volta completata la migrazione, viene stabilita una nuova connessione utilizzando la nuova porta dati.

Se il criterio di failover non è configurato per migrare la porta dati, il server FPolicy deve attendere che venga visualizzato il nodo guasto. Una volta attivato il nodo, viene avviata una nuova connessione da quel nodo con un nuovo ID sessione.

> Il server FPolicy rileva le connessioni interrotte con il messaggio del protocollo Keep-alive. Il timeout per l'eliminazione dell'ID sessione viene determinato durante la configurazione di FPolicy. Il timeout di mantenimento predefinito è di due minuti.

Come funzionano i servizi FPolicy negli spazi dei nomi SVM

ONTAP offre uno spazio dei nomi di una macchina virtuale di storage unificata (SVM). I volumi nel cluster vengono Uniti da giunzioni per fornire un singolo file system logico. Il server FPolicy è a conoscenza della topologia dello spazio dei nomi e fornisce i servizi FPolicy attraverso lo spazio dei nomi.

Lo spazio dei nomi è specifico e contenuto all'interno di SVM; pertanto, è possibile visualizzare lo spazio dei nomi solo dal contesto SVM. Gli spazi dei nomi hanno le seguenti caratteristiche:

- In ogni SVM esiste un singolo namespace, con la radice dello spazio dei nomi come volume root, rappresentata nello spazio dei nomi come barra (/).
- Tutti gli altri volumi hanno punti di giunzione sotto la radice (/).
- Le giunzioni dei volumi sono trasparenti per i client.
- Una singola esportazione NFS può fornire l'accesso all'intero namespace; in caso contrario, le policy di esportazione possono esportare volumi specifici.
- Le condivisioni SMB possono essere create sul volume o su qtree all'interno del volume o su qualsiasi directory all'interno dello spazio dei nomi.
- L'architettura dello spazio dei nomi è flessibile.

  Di seguito sono riportati alcuni esempi di architetture di namespace tipiche:

  - Uno spazio dei nomi con una singola diramazione fuori dalla directory principale
  - Uno spazio dei nomi con più diramazioni al di fuori della radice
  - Uno spazio dei nomi con più volumi non ramificati fuori dalla directory principale

In che modo FPolicy pass-through-Read migliora l'usabilità per la gestione dello storage gerarchico

La funzione pass-through-Read consente al server FPolicy (che funge da server HSM) di fornire l'accesso in lettura ai file offline senza dover richiamare il file dal sistema di storage secondario al sistema di storage primario.

Quando un server FPolicy è configurato per fornire HSM ai file che risiedono su un server SMB, si verifica una migrazione dei file basata su policy in cui i file sono memorizzati offline sullo storage secondario e solo un file stub rimane sullo storage primario. Anche se un file stub viene visualizzato come un file normale per i client, in realtà è un file sparse che ha le stesse dimensioni del file originale. Il file sparse ha il bit SMB offline impostato e punta al file effettivo che è stato migrato allo storage secondario.

In genere, quando si riceve una richiesta di lettura per un file offline, il contenuto richiesto deve essere richiamato allo storage primario e quindi accessibile attraverso lo storage primario. La necessità di richiamare i dati sullo storage primario ha diversi effetti indesiderati. Tra gli effetti indesiderati vi è la maggiore latenza per le richieste dei client causata dalla necessità di richiamare il contenuto prima di rispondere alla richiesta e l'aumento del consumo di spazio necessario per i file richiamati sullo storage primario.

FPolicy pass-through-Read consente al server HSM (il server FPolicy) di fornire l'accesso in lettura ai file migrati offline senza dover richiamare il file dal sistema di storage secondario al sistema di storage primario. Invece di richiamare i file sullo storage primario, le richieste di lettura possono essere gestite direttamente dallo storage secondario.

L'offload della copia (ODX) non è supportato con l'operazione di pass-through-lettura FPolicy.

La lettura pass-through migliora l'usabilità fornendo i seguenti vantaggi:

- Le richieste di lettura possono essere gestite anche se lo storage primario non dispone di spazio sufficiente per richiamare i dati richiesti nello storage primario.
- Migliore gestione della capacità e delle performance in caso di aumento del richiamo dei dati, ad esempio se uno script o una soluzione di backup necessita di accedere a molti file offline.
- Le richieste di lettura per i file offline nelle copie Snapshot possono essere gestite.

  Poiché le copie Snapshot sono di sola lettura, il server FPolicy non può ripristinare il file originale se il file stub si trova in una copia Snapshot. L'utilizzo di pass-through-Read elimina questo problema.

- È possibile impostare policy che controllano quando le richieste di lettura vengono gestite attraverso l'accesso al file sullo storage secondario e quando il file offline deve essere richiamato sullo storage primario.

  Ad esempio, è possibile creare un criterio sul server HSM che specifica il numero di volte in cui è possibile accedere al file offline in un determinato periodo di tempo prima che il file venga nuovamente migrato nello storage primario. Questo tipo di policy evita di richiamare i file a cui si accede raramente.

Come vengono gestite le richieste di lettura quando FPolicy pass-through-Read è attivato

È necessario comprendere come vengono gestite le richieste di lettura quando FPolicy pass-through-Read è attivato, in modo da poter configurare in modo ottimale la connettività tra la macchina virtuale di storage (SVM) e i server FPolicy.

Quando FPolicy pass-through-Read è attivato e la SVM riceve una richiesta di un file offline, FPolicy invia una notifica al server FPolicy (server HSM) attraverso il canale di connessione standard.

Dopo aver ricevuto la notifica, il server FPolicy legge i dati dal percorso del file inviato nella notifica e invia i dati richiesti alla SVM attraverso la connessione dati privilegiata pass-through-Read stabilita tra la SVM e il server FPolicy.

Una volta inviati i dati, il server FPolicy risponde alla richiesta di lettura come ALLOW (CONSENTI) o DENY (RIFIUTA). A seconda che la richiesta di lettura sia consentita o rifiutata, ONTAP invia le informazioni richieste o invia un messaggio di errore al client.

Pianificare la configurazione di FPolicy

Requisiti, considerazioni e Best practice per la configurazione di FPolicy

Prima di creare e configurare le configurazioni FPolicy sulle SVM, è necessario conoscere alcuni 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 LIF client per le connessioni FPolicy in uscita con l'aggiunta di `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.
- 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.

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.

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

Contatori	Descrizione
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
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.

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 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.

4. 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.

5. 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 (motore esterno), è necessario comprendere il significato della creazione di 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 effettuare e gestire le connessioni ai server FPolicy esterni (server FPolicy), incluse le seguenti informazioni:

- 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
- 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`
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 e NFSv4.

- 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.	`-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.	`-filters filter, ...`

Filtri (continua) • `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 del client per la modifica del DACL in un file o in una directory. Questo filtro è disponibile solo per i protocolli SMB e NFSv4. • `setattr-with-modify-time-change` opzione per filtrare le richieste setattr del client per modificare l'ora di modifica di un file o di una directory. • `setattr-with-access-time-change` opzione per filtrare le richieste setattr del client per modificare l'ora di accesso di un file o di una directory. • `setattr-with-creation-time-change` opzione per filtrare le richieste setattr del client per modificare l'ora di creazione di un file o di una directory. Questa opzione è disponibile solo per il protocollo SMB. • `setattr-with-mode-change` opzione per filtrare le richieste setattr del client per modificare i bit di modalità su un file o una directory. • `setattr-with-size-change` opzione per filtrare le richieste setattr del client per modificare le dimensioni di un file. • `setattr-with-allocation-size-change` opzione per filtrare le richieste setattr del client per modificare la dimensione di allocazione di un file. Questa opzione è disponibile solo per il protocollo SMB. • `exclude-directory` opzione per filtrare le richieste del client per le operazioni di directory. Quando viene specificato questo filtro, le operazioni della directory non vengono monitorate.	`-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.

L'elenco delle operazioni di file supportate e delle combinazioni di filtri per il monitoraggio FPolicy degli eventi di accesso al file NFSv4 è riportato nella seguente tabella:

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 operazioni di accesso negato supportate per il monitoraggio FPolicy degli eventi di accesso al file NFSv4 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
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

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`, il 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.

- Se si desidera configurare pass-through-Read, è necessario configurare anche il criterio in modo da consentire l'accesso con privilegi.

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	
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		

Creare la configurazione FPolicy

Creare il motore esterno 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.

Di cosa hai bisogno

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
   ```

   ```
                                   Primary        Secondary
   External
   Vserver            Engine       Servers        Servers       Port Engine
   Type
   ---------------    -----------  -------------- ----------- ------
   -----------
   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: -
   ```

Creare l’evento 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

Devi 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
   ```

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

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
   ```

Creare archivi persistenti

A partire da ONTAP 9.14.1, FPolicy consente di impostare un "Archivi persistenti" 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.

Best practice

- Prima di utilizzare la funzionalità di archivio permanente, assicurati che le tue applicazioni partner supportino questa configurazione.

- Il volume dello storage persistente viene configurato in base alle singole SVM. Per ogni SVM abilitata per FPolicy avrai bisogno di un volume archivio persistente.
- Il nome del volume di archiviazione persistente e il percorso di giunzione specificati al momento della creazione del volume dovrebbero corrispondere.
- Crea il volume di archivio persistente sul nodo con LIF che prevedono il monitoraggio del traffico massimo da parte di Fpolicy.
- Impostare il criterio snapshot su `none` per quel volume 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.
- 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. Per ottenere questo risultato, dopo aver attivato FPolicy, smontare il volume in ONTAP per rimuovere il percorso di giunzione; ciò lo rende inaccessibile per l'accesso al protocollo utente.

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> -junction
   -path <path> -policy <default> -unix-permissions <777> -size <value>
   -aggregate <aggregate name> -snapshot-policy <none>
   ```

   - Le dimensioni del volume dell'archivio persistente si basano sul periodo di tempo per il quale si desidera mantenere gli eventi non inviati 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 x 30 x 60 x 0,6KB (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`.

   - Si prevede che un utente amministratore con privilegi RBAC sufficienti (per creare un volume) creerà un volume (utilizzando il comando cli di volume o l'API REST) della dimensione desiderata e fornirà il nome di quel volume come `-volume` Nell'archivio persistente creare un comando CLI o API REST.
2. Creare l'archivio persistente:

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

   - Persistent-store: Il nome dell'archivio persistente
   - Volume: Il volume della memoria persistente
3. Dopo aver creato l'archivio persistente, è possibile creare il criterio FPolicy e aggiungere il nome dell'archivio persistente a tale criterio. Per ulteriori informazioni, vedere "Creare il criterio FPolicy".

Creare il criterio 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.

Di cosa hai bisogno

- 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     Events    Engine    Is Mandatory  Privileged
                 Name                                         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
```

Creare l'ambito 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.

Di cosa hai bisogno

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: -
```

Attivare il criterio 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.

Di cosa hai bisogno

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

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

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

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

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

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

Gestire le configurazioni FPolicy

Modificare le configurazioni FPolicy

Comandi per la modifica delle configurazioni FPolicy

È possibile modificare le configurazioni FPolicy modificando gli elementi che compongono la configurazione. È possibile modificare motori esterni, eventi FPolicy, ambiti FPolicy e policy FPolicy. È inoltre possibile attivare o disattivare i criteri FPolicy. Quando si disattiva il criterio FPolicy, il monitoraggio dei file viene interrotto per tale criterio.

Si consiglia di disattivare il criterio FPolicy prima di modificare la configurazione.

Se si desidera modificare…	Utilizzare questo comando…
Motori esterni	`vserver fpolicy policy external-engine modify`
Eventi	`vserver fpolicy policy event modify`
Ambiti	`vserver fpolicy policy scope modify`
Policy	`vserver fpolicy policy modify`

Per ulteriori informazioni, vedere le pagine man per i comandi.

Attivare o disattivare i criteri FPolicy

Una volta completata la configurazione, è possibile attivare i criteri FPolicy. L'abilitazione del criterio determina la priorità e avvia il monitoraggio dell'accesso al file per il criterio. È possibile disattivare i criteri FPolicy se si desidera interrompere il monitoraggio dell'accesso ai file per il criterio.

Di cosa hai bisogno

Prima di attivare i criteri FPolicy, è necessario completare la configurazione 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.
- Se si desidera modificare la priorità di un criterio FPolicy, è necessario disattivarlo e riattivarlo utilizzando il nuovo numero di sequenza.

Fase

1. Eseguire l'azione appropriata:

Se si desidera…	Immettere il seguente comando…
Attivare un criterio FPolicy	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`
Disattiva un criterio FPolicy	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

Visualizza informazioni sulle configurazioni FPolicy

Funzionamento dei comandi di visualizzazione

Durante la visualizzazione delle informazioni sulla configurazione di FPolicy, è utile comprendere come `show` i comandi funzionano.

R `show` il comando senza parametri aggiuntivi visualizza le informazioni in un modulo riepilogativo. Inoltre, ogni `show` il comando ha gli stessi due parametri opzionali che si escludono a vicenda, `-instance` e. `-fields`.

Quando si utilizza `-instance` parametro con a. `show` l'output del comando visualizza informazioni dettagliate in un formato di elenco. In alcuni casi, l'output dettagliato può essere lungo e includere più informazioni di quante ne hai bisogno. È possibile utilizzare `-fields fieldname[,fieldname…]` parametro per personalizzare l'output in modo che visualizzi le informazioni solo per i campi specificati. È possibile identificare i campi che è possibile specificare immettendo `?` dopo il `-fields` parametro.

> L'output di un `show` con il `-fields` il parametro potrebbe visualizzare altri campi pertinenti e necessari relativi ai campi richiesti.

Ogni `show` command dispone di uno o più parametri opzionali che filtrano l'output e consentono di limitare l'ambito delle informazioni visualizzate nell'output del comando. È possibile identificare i parametri opzionali disponibili per un comando immettendo `?` dopo il `show` comando.

Il `show` Il comando supporta i modelli e i caratteri jolly in stile UNIX per consentire la corrispondenza di più valori negli argomenti dei parametri di comando. Ad esempio, è possibile utilizzare l'operatore jolly (*), L'operatore NOT (!), L'operatore OR (|), l'operatore di intervallo (integer…integer), l'operatore meno di (<), l'operatore maggiore di (>), l'operatore minore o uguale a (⇐) e maggiore o uguale all'operatore (>=) quando si specificano i valori.

Per ulteriori informazioni sull'utilizzo di modelli e caratteri jolly in stile UNIX, vedere Utilizzando l'interfaccia della riga di comando di ONTAP.

Comandi per la visualizzazione delle informazioni sulle configurazioni FPolicy

Si utilizza `fpolicy show` Comandi per visualizzare informazioni sulla configurazione di FPolicy, incluse informazioni su motori esterni, eventi, ambiti e policy di FPolicy.

Se si desidera visualizzare informazioni su FPolicy…	Utilizzare questo comando…

Motori esterni	`vserver fpolicy policy external-engine show`
Eventi	`vserver fpolicy policy event show`
Ambiti	`vserver fpolicy policy scope show`
Policy	`vserver fpolicy policy show`

Per ulteriori informazioni, vedere le pagine man per i comandi.

Visualizza informazioni sullo stato dei criteri FPolicy

È possibile visualizzare informazioni sullo stato dei criteri FPolicy per determinare se un criterio è abilitato, quale motore esterno è configurato per l'utilizzo, quale numero di sequenza corrisponde al criterio e a quale SVM (Storage Virtual Machine) è associato il criterio FPolicy.

A proposito di questa attività

Se non si specificano parametri, il comando visualizza le seguenti informazioni:

- Nome SVM
- Nome policy
- Numero di sequenza del criterio
- Stato della policy

Oltre a visualizzare le informazioni sullo stato dei criteri per i criteri FPolicy configurati sul cluster o su una SVM specifica, è possibile utilizzare i parametri dei comandi per filtrare l'output del comando in base ad altri criteri.

È possibile specificare `-instance` parametro per visualizzare informazioni dettagliate sui criteri elencati. In alternativa, è possibile utilizzare `-fields` per visualizzare solo i campi indicati nell'output del comando, o. `-fields ?` per determinare quali campi è possibile utilizzare.

Fase

1. Visualizzare le informazioni filtrate sullo stato dei criteri FPolicy utilizzando il comando appropriato:

Se si desidera visualizzare le informazioni di stato relative ai criteri…	Immettere il comando…
Sul cluster	`vserver fpolicy show`
Che hanno lo stato specificato	`vserver fpolicy show -status {on
off}`	Su una SVM specificata

`vserver fpolicy show -vserver vserver_name`	Con il nome del criterio specificato
`vserver fpolicy show -policy-name policy_name`	Che utilizzano il motore esterno specificato

Esempio

Nell'esempio seguente vengono visualizzate le informazioni relative ai criteri FPolicy nel cluster:

```
cluster1::> vserver fpolicy show
                                          Sequence
Vserver             Policy Name             Number  Status      Engine
------------------- ------------------- --------  ---------   ---------
FPolicy             cserver_policy      -         off         eng1
vs1.example.com     v1p1                -         off         eng2
vs1.example.com     v1p2                -         off         native
vs1.example.com     v1p3                -         off         native
vs1.example.com     cserver_policy      -         off         eng1
vs2.example.com     v1p1                3         on          native
vs2.example.com     v1p2                1         on          eng3
vs2.example.com     cserver_policy      2         on          eng1
```

Visualizza informazioni sui criteri FPolicy abilitati

È possibile visualizzare informazioni sui criteri FPolicy abilitati per determinare il motore esterno FPolicy configurato per l'utilizzo, la priorità del criterio e la macchina virtuale dello storage (SVM) a cui è associato il criterio FPolicy.

A proposito di questa attività

Se non si specificano parametri, il comando visualizza le seguenti informazioni:

- Nome SVM
- Nome policy
- Priorità della policy

È possibile utilizzare i parametri dei comandi per filtrare l'output del comando in base a criteri specifici.

Fase

1. Visualizzare le informazioni sui criteri FPolicy abilitati utilizzando il comando appropriato:

Se si desidera visualizzare informazioni sui criteri abilitati…	Immettere il comando…
Sul cluster	`vserver fpolicy show-enabled`

Su una SVM specificata	`vserver fpolicy show-enabled -vserver vserver_name`
Con il nome del criterio specificato	`vserver fpolicy show-enabled -policy-name policy_name`
Con il numero di sequenza specificato	`vserver fpolicy show-enabled -priority integer`

Esempio

Nell'esempio seguente vengono visualizzate le informazioni relative ai criteri FPolicy abilitati sul cluster:

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

Gestire le connessioni del server FPolicy

Connettersi a server FPolicy esterni

Per attivare l'elaborazione dei file, potrebbe essere necessario connettersi manualmente a un server FPolicy esterno se la connessione è stata interrotta in precedenza. Una connessione viene interrotta dopo il timeout del server o a causa di un errore. In alternativa, l'amministratore potrebbe interrompere manualmente una connessione.

A proposito di questa attività

Se si verifica un errore irreversibile, la connessione al server FPolicy può essere interrotta. Dopo aver risolto il problema che ha causato l'errore irreversibile, è necessario riconnettersi manualmente al server FPolicy.

Fasi

1. Connettersi al server FPolicy esterno utilizzando `vserver fpolicy engine-connect` comando.

   Per ulteriori informazioni sul comando, vedere le pagine man.

2. Verificare che il server FPolicy esterno sia connesso utilizzando `vserver fpolicy show-engine` comando.

   Per ulteriori informazioni sul comando, vedere le pagine man.

Disconnettersi dai server FPolicy esterni

Potrebbe essere necessario disconnettersi manualmente da un server FPolicy esterno.

Ciò potrebbe essere utile se il server FPolicy ha problemi con l'elaborazione della richiesta di notifica o se è necessario eseguire la manutenzione sul server FPolicy.

Fasi

1. Disconnettersi dal server FPolicy esterno utilizzando `vserver fpolicy engine-disconnect` comando.

   Per ulteriori informazioni sul comando, vedere le pagine man.

2. Verificare che il server FPolicy esterno sia disconnesso utilizzando `vserver fpolicy show-engine` comando.

   Per ulteriori informazioni sul comando, vedere le pagine man.

Visualizza informazioni sulle connessioni a server FPolicy esterni

È possibile visualizzare informazioni sullo stato delle connessioni a server FPolicy esterni (server FPolicy) per il cluster o per una specifica macchina virtuale di storage (SVM). Queste informazioni consentono di determinare quali server FPolicy sono connessi.

A proposito di questa attività

Se non si specificano parametri, il comando visualizza le seguenti informazioni:

- Nome SVM
- Nome del nodo
- Nome del criterio FPolicy
- Indirizzo IP del server FPolicy
- Stato del server FPolicy
- Tipo di server FPolicy

Oltre a visualizzare informazioni sulle connessioni FPolicy sul cluster o su una specifica SVM, è possibile utilizzare i parametri dei comandi per filtrare l'output del comando in base ad altri criteri.

È possibile specificare `-instance` parametro per visualizzare informazioni dettagliate sui criteri elencati. In alternativa, è possibile utilizzare `-fields` parametro per visualizzare solo i campi indicati nell'output del comando. È possibile immettere `?` dopo il `-fields` parametro per scoprire quali campi è possibile utilizzare.

Fase

1. Visualizzare le informazioni filtrate sullo stato della connessione tra il nodo e il server FPolicy utilizzando il comando appropriato:

Se si desidera visualizzare le informazioni sullo stato della connessione relative ai server FPolicy…	Inserisci…
Specificato dall'utente	`vserver fpolicy show-engine -server IP_address`

Per una SVM specificata	`vserver fpolicy show-engine -vserver vserver_name`
Che sono associati a una policy specificata	`vserver fpolicy show-engine -policy-name policy_name`
Con lo stato del server specificato	`vserver fpolicy show-engine -server-status status` Lo stato del server può essere uno dei seguenti: • `connected` • `disconnected` • `connecting` • `disconnecting`
Con il tipo specificato	`vserver fpolicy show-engine -server-type type` Il tipo di server FPolicy può essere uno dei seguenti: • `primary` • `secondary`
Disconnessi con il motivo specificato	`vserver fpolicy show-engine -disconnect-reason text` La disconnessione può essere dovuta a diversi motivi. Di seguito sono riportati i motivi più comuni per la disconnessione: • `Disconnect command received from CLI.` • `Error encountered while parsing notification response from FPolicy server.` • `FPolicy Handshake failed.` • `SSL handshake failed.` • `TCP Connection to FPolicy server failed.` • `The screen response message received from the FPolicy server is not valid.`

Esempio

Questo esempio mostra informazioni sulle connessioni esterne del motore ai server FPolicy su SVM vs1.example.com:

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                                Server-       Server-
Vserver         Policy    Node         Server        status        type
--------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1   node1        10.1.1.2      connected     primary
vs1.example.com policy1   node1        10.1.1.3      disconnected  primary
vs1.example.com policy1   node2        10.1.1.2      connected     primary
vs1.example.com policy1   node2        10.1.1.3      disconnected  primary
```

Nell'esempio riportato di seguito vengono visualizzate solo informazioni relative ai server FPolicy connessi:

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver         policy-name server
---------- --------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2
```

Visualizza le informazioni sullo stato della connessione pass-through-Read di FPolicy

È possibile visualizzare informazioni sullo stato della connessione pass-through-Read di FPolicy ai server FPolicy esterni (server FPolicy) per il cluster o per una specifica macchina virtuale di storage (SVM). Queste informazioni consentono di determinare quali server FPolicy dispongono di connessioni dati pass-through-Read e per quali server FPolicy la connessione pass-through-Read è disconnessa.

A proposito di questa attività

Se non si specifica alcun parametro, il comando visualizza le seguenti informazioni:

- Nome SVM
- Nome del criterio FPolicy
- Nome del nodo
- Indirizzo IP del server FPolicy
- Stato della connessione pass-through-Read di FPolicy

Oltre a visualizzare informazioni sulle connessioni FPolicy sul cluster o su una specifica SVM, è possibile utilizzare i parametri dei comandi per filtrare l'output del comando in base ad altri criteri.

È possibile specificare `-instance` parametro per visualizzare informazioni dettagliate sui criteri elencati. In alternativa, è possibile utilizzare `-fields` parametro per visualizzare solo i campi indicati nell'output del comando. È possibile immettere `?` dopo il `-fields` parametro per scoprire quali campi è possibile utilizzare.

Fase

1. Visualizzare le informazioni filtrate sullo stato della connessione tra il nodo e il server FPolicy utilizzando il

comando appropriato:

Se si desidera visualizzare le informazioni sullo stato della connessione relative a…	Immettere il comando…
Stato della connessione pass-through-Read FPolicy per il cluster	`vserver fpolicy show-passthrough-read-connection`
Stato della connessione pass-through-Read FPolicy per una SVM specificata	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`
Stato della connessione pass-through-Read FPolicy per una policy specifica	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
Stato dettagliato della connessione pass-through-Read di FPolicy per una policy specifica	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`
Stato della connessione passthrough-Read FPolicy per lo stato specificato	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status` Lo stato del server può essere uno dei seguenti: • `connected` • `disconnected`

Esempio

Il seguente comando visualizza informazioni sulle connessioni pass-through-Read da tutti i server FPolicy del cluster:

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                            FPolicy           Server
Vserver          Policy Name   Node         Server            Status
---------------  ------------- ------------ -----------------
--------------
vs2.example.com  pol_cifs_2    FPolicy-01   2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
```

Il seguente comando visualizza informazioni dettagliate sulle connessioni pass-through-Read dai server FPolicy configurati nel criterio “pol_cifs_1”:

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                             Node: FPolicy-01
                                          Vserver: vs1.example.com
                                           Policy: pol_cifs_1
                                           Server: 1.1.1.1
                 Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                     Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```