Sicurezza e crittografia dei dati

ONTAP 9

NetApp
April 24, 2024

Sommario

Sicurezza e crittografia dei dati

Panoramica sulla gestione della sicurezza con System Manager

A partire da ONTAP 9.7, è possibile gestire la sicurezza del cluster con Gestione di sistema.

Con Gestione sistema, si utilizzano i metodi standard di ONTAP per proteggere l'accesso client e amministratore allo storage e per proteggerlo dai virus. Sono disponibili tecnologie avanzate per la crittografia dei dati a riposo e per lo storage WORM.

Se si utilizza la gestione di sistema classica (disponibile solo in ONTAP 9.7 e versioni precedenti), fare riferimento a. "System Manager Classic (ONTAP da 9.0 a 9.7)"

Scansione virus

È possibile utilizzare la funzionalità antivirus integrata nel sistema di storage per proteggere i dati da virus o altri codici dannosi. La scansione antivirus di ONTAP, denominata *Vscan*, combina il software antivirus di terze parti più all'avanguardia con le funzionalità di ONTAP che offrono la flessibilità necessaria per controllare quali file vengono sottoposti a scansione e quando.

Crittografia

ONTAP offre tecnologie di crittografia basate su software e hardware per garantire che i dati inattivi non possano essere letti in caso di riposizionamento, restituzione, smarrimento o furto del supporto di storage.

Storage WORM

SnapLock è una soluzione per la compliance dalle performance elevate per le organizzazioni che utilizzano lo storage *write once*, *Read Many (WORM)* per conservare i file critici in forma non modificata per scopi normativi e di governance.

Proteggersi dal ransomware

Panoramica della protezione ransomware autonoma

A partire da ONTAP 9.10.1, la funzionalità di protezione ransomware autonoma (ARP) utilizza l'analisi del carico di lavoro in ambienti NAS (NFS e SMB) per rilevare e avvisare in modo proattivo circa attività anomale che potrebbero indicare un attacco ransomware.

Quando si sospetta un attacco, ARP crea anche nuove copie Snapshot, oltre alla protezione esistente dalle copie Snapshot pianificate.

Licenze e abilitazione

ARP richiede una licenza. ARP è disponibile con "Licenza ONTAP ONE". Se non si dispone della licenza ONTAP ONE, sono disponibili altre licenze per l'utilizzo di ARP, che variano a seconda della versione di ONTAP in uso.

Release di ONTAP	Licenza
ONTAP 9.11.1 e versioni successive	Anti_ransomware
ONTAP 9.10.1	MT_EK_MGMT (Gestione delle chiavi multi-tenant)

- Se si esegue l'aggiornamento a ONTAP 9.11.1 o versione successiva e ARP è già configurato nel sistema, non è necessario acquistare la nuova licenza Anti-ransomware. Per le nuove configurazioni ARP, è necessaria la nuova licenza.
- Se si esegue il ripristino da ONTAP 9.11.1 o versione successiva a ONTAP 9.10.1 e si attiva ARP con la licenza Anti-ransomware, viene visualizzato un messaggio di avviso e potrebbe essere necessario riconfigurare ARP. "Scopri come ripristinare ARP".

È possibile configurare ARP per volume utilizzando Gestione sistema o l'interfaccia CLI di ONTAP.

Strategia di protezione ransomware di ONTAP

Una strategia efficace di rilevamento ransomware dovrebbe includere più di un singolo livello di protezione.

Un'analogia sarebbe la sicurezza di un veicolo. Non ci si affida a una singola funzione, ad esempio una cintura di sicurezza, per proteggersi completamente in caso di incidente. Gli airbag, i freni antibloccaggio e l'allarme anticollisione anteriore sono tutte funzioni di sicurezza aggiuntive che consentono di ottenere risultati migliori. La protezione ransomware deve essere visualizzata nello stesso modo.

Mentre ONTAP include funzionalità come FPolicy, Snapshot Copies, SnapLock e Active IQ Digital Advisor per la protezione dal ransomware, le seguenti informazioni si concentrano sulla funzionalità ARP on-box con funzionalità di machine learning.

Per ulteriori informazioni sulle altre funzionalità anti-ransomware di ONTAP, consulta la sezione "TR-4572: Soluzione NetApp per ransomware."

Cosa rileva ARP

ARP è progettato per proteggere da attacchi di tipo Denial-of-service in cui l'utente malintenzionato trattiene i dati fino a quando non viene pagato un riscatto. ARP offre il rilevamento anti-ransomware basato su:

- Identificazione dei dati in entrata come crittografati o non crittografati.
- Analytics, che rileva
  - **Entropia**: Una valutazione della casualità dei dati in un file
  - **Tipi di estensione del file**: Un'estensione non conforme al normale tipo di estensione
  - **IOPS del file**: Aumento dell'attività anomala del volume con crittografia dei dati (a partire da ONTAP 9.11.1)

ARP è in grado di rilevare la diffusione della maggior parte degli attacchi ransomware dopo la crittografia di un numero limitato di file, intraprendere azioni automatiche per proteggere i dati e avvisare l'utente che si sta verificando un attacco sospetto.

> Nessun sistema di rilevamento ransomware o prevenzione può garantire completamente la sicurezza da un attacco ransomware. Anche se è possibile che un attacco possa non essere rilevato, ARP agisce come un importante livello di difesa aggiuntivo se il software antivirus non è riuscito a rilevare un'intrusione.

Modalità di apprendimento e attive

ARP dispone di due modalità:

- **Apprendimento** (o modalità "dry run")
- **Attivo** (o modalità "abilitato")

Quando si attiva ARP, viene eseguito in *modalità di apprendimento*. In modalità di apprendimento, il sistema ONTAP sviluppa un profilo di avviso basato sulle aree di analisi: Entropia, tipi di estensione dei file e IOPS dei file. Dopo aver eseguito ARP in modalità di apprendimento per un tempo sufficiente a valutare le caratteristiche del carico di lavoro, è possibile passare alla modalità attiva e iniziare a proteggere i dati. Una volta che ARP è passato alla modalità attiva, ONTAP crea copie snapshot ARP per proteggere i dati se viene rilevata una minaccia.

Si consiglia di lasciare ARP in modalità di apprendimento per 30 giorni. A partire da ONTAP 9.13.1, ARP determina automaticamente l'intervallo ottimale del periodo di apprendimento e automatizza lo switch, che può verificarsi prima di 30 giorni.

In modalità attiva, se un'estensione del file è contrassegnata come anomala, è necessario valutare l'avviso. Puoi agire sull'avviso per proteggere i tuoi dati o contrassegnarlo come falso positivo. Se si contrassegna un avviso come falso positivo, il profilo di avviso viene aggiornato. Ad esempio, se l'avviso viene attivato da una nuova estensione di file e l'utente contrassegna l'avviso come falso positivo, non verrà visualizzato alcun avviso alla successiva visualizzazione dell'estensione del file. Il comando `security anti-ransomware volume workload-behavior show` mostra le estensioni di file rilevate nel volume. (Se si esegue questo comando nelle prime fasi della modalità di apprendimento e viene visualizzata una rappresentazione accurata dei tipi di file, non utilizzare tali dati come base per passare alla modalità attiva, poiché ONTAP sta ancora raccogliendo altre metriche).

A partire da ONTAP 9.11.1, è possibile personalizzare i parametri di rilevamento per ARP. Per ulteriori informazioni, vedere Gestire i parametri di rilevamento degli attacchi ARP.

Valutazione delle minacce e copie snapshot ARP

In modalità attiva, ARP valuta la probabilità di minaccia in base ai dati in entrata misurati in base alle analisi apprese. Viene assegnata una misurazione quando ARP rileva una minaccia:

- **Basso**: Il primo rilevamento di un'anomalia nel volume (ad esempio, una nuova estensione del file è osservata nel volume).
- **Moderato**: Si osservano più file con la stessa estensione mai vista prima.
  - In ONTAP 9.10.1, la soglia per l'escalation a moderate è di 100 o più file. A partire da ONTAP 9.11.1, è possibile modificare la quantità di file; il valore predefinito è 20.

In una situazione di basso rischio, ONTAP rileva un'anomalia e crea una copia Snapshot del volume per creare il punto di recovery migliore. ONTAP anticipa il nome della copia snapshot ARP con `Anti-ransomware-backup` per renderla facilmente identificabile, per esempio `Anti_ransomware_backup.2022-12-20_1248`.

Dopo che ONTAP ha eseguito un report di analytics, la minaccia passa a moderata. Ciò determina se l'anomalia corrisponde a un profilo ransomware. Le minacce che rimangono a basso livello sono registrate e visibili nella sezione **Eventi** di System Manager. Quando la probabilità di attacco è moderata, ONTAP genera una notifica EMS che richiede di valutare la minaccia. ONTAP non invia avvisi relativi a minacce basse, tuttavia, a partire da ONTAP 9.14.1, è possibile modificare le impostazioni degli avvisi. Per ulteriori informazioni, vedere Rispondere ad attività anomale.

È possibile visualizzare informazioni su una minaccia, indipendentemente dal livello, nella sezione **Eventi** di System Manager o con `security anti-ransomware volume show` comando.

Le copie Snapshot ARP vengono conservate per un minimo di due giorni. A partire da ONTAP 9.11.1, è possibile modificare le impostazioni di conservazione. Per ulteriori informazioni, vedere Modificare le opzioni per le copie Snapshot.

Come ripristinare i dati in ONTAP dopo un attacco ransomware

Quando si sospetta un attacco, il sistema esegue una copia Snapshot del volume in quel momento e blocca tale copia. Se l'attacco viene confermato in seguito, il volume può essere ripristinato utilizzando la copia snapshot ARP.

Le copie Snapshot bloccate non possono essere eliminate con mezzi normali. Tuttavia, se in seguito decidi di contrassegnare l'attacco come falso positivo, la copia bloccata verrà eliminata.

Conoscendo i file interessati e il momento dell'attacco, è possibile recuperare in modo selettivo i file interessati da varie copie Snapshot, piuttosto che semplicemente riportare l'intero volume in una delle copie Snapshot.

ARP si basa quindi sulla comprovata tecnologia di protezione dei dati e disaster recovery di ONTAP per rispondere agli attacchi ransomware. Per ulteriori informazioni sul ripristino dei dati, consultare i seguenti argomenti.

- "Ripristino da copie Snapshot (System Manager)"
- "Ripristino dei file da copie Snapshot (CLI)"
- "Ripristino ransomware intelligente"

Casi di utilizzo e considerazioni sulla protezione ransomware autonoma

La protezione autonoma ransomwware (ARP) è disponibile per i carichi di lavoro NAS a partire da ONTAP 9.10.1. Prima di distribuire ARP, è necessario conoscere gli utilizzi consigliati e le configurazioni supportate, nonché le implicazioni in termini di prestazioni.

Configurazioni supportate e non supportate

Quando si decide di utilizzare l'ARP, è importante assicurarsi che il carico di lavoro del volume sia adatto all'ARP e che soddisfi le configurazioni di sistema richieste.

Carichi di lavoro adatti

ARP è adatto per:

- Database sullo storage NFS
- Home directory Windows o Linux

  Poiché gli utenti potrebbero creare file con estensioni che non sono state rilevate durante il periodo di apprendimento, esiste una maggiore possibilità di falsi positivi in questo carico di lavoro.

- Immagini e video

  Ad esempio, le cartelle cliniche e i dati EDA (Electronic Design Automation)

Carichi di lavoro non adatti

ARP non è adatto per:

- Carichi di lavoro con un'elevata frequenza di creazione o eliminazione di file (centinaia di migliaia di file in pochi secondi, ad esempio workload di test/sviluppo).
- Il rilevamento delle minacce di ARP dipende dalla sua capacità di riconoscere un aumento insolito delle attività di creazione, ridenominazione o eliminazione dei file. Se l'applicazione stessa è l'origine dell'attività del file, non è possibile distinguerla in modo efficace dall'attività ransomware.
- Carichi di lavoro in cui l'applicazione o l'host crittografa i dati.
  ARP dipende dalla distinzione dei dati in entrata come crittografati o non crittografati. Se l'applicazione stessa sta crittografando i dati, l'efficacia della funzione viene ridotta. Tuttavia, la funzionalità può ancora funzionare in base all'attività del file (eliminazione, sovrascrittura o creazione, creazione o ridenominazione con una nuova estensione del file) e al tipo di file.

Configurazioni supportate

ARP è disponibile per i volumi NFS e SMB nei sistemi ONTAP on-premise a partire da ONTAP 9.10.1.

Il supporto per altre configurazioni e tipi di volume è disponibile nelle seguenti versioni di ONTAP:

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Volumi protetti con SnapMirror asincrono	✓	✓	✓		
SVM protette con SnapMirror asincrono (disaster recovery SVM)	✓	✓	✓		
Mobilità dei dati SVM (`vserver migrate`)	✓	✓	✓		
Volumi FlexGroup	✓	✓			
Verifica multi-admin	✓	✓			

Interoperabilità di SnapMirror e ARP

A partire da ONTAP 9.12.1, ARP è supportato sui volumi di destinazione asincroni di SnapMirror. ARP è **non** supportato con SnapMirror Synchronous.

Se un volume di origine SnapMirror è abilitato per ARP, il volume di destinazione SnapMirror acquisisce automaticamente lo stato di configurazione ARP (apprendimento, abilitato, ecc.), i dati di training ARP e l'istantanea creata da ARP del volume di origine. Non è richiesta alcuna abilitazione esplicita.

Mentre il volume di destinazione è costituito da copie Snapshot di sola lettura (RO), non viene eseguita alcuna elaborazione ARP sui dati. Tuttavia, quando il volume di destinazione di SnapMirror viene convertito in lettura/scrittura (RW), ARP viene attivato automaticamente sul volume di destinazione convertito in RW. Il volume di destinazione non richiede ulteriori procedure di apprendimento oltre a quelle già registrate nel

volume di origine.

In ONTAP 9.10.1 e 9.11.1, SnapMirror non trasferisce lo stato di configurazione ARP, i dati di training e le copie Snapshot dai volumi di origine a quelli di destinazione. Quindi, quando il volume di destinazione SnapMirror viene convertito in RW, ARP sul volume di destinazione deve essere esplicitamente abilitato in modalità di apprendimento dopo la conversione.

ARP e macchine virtuali

ARP è supportato con macchine virtuali (VM). Il rilevamento ARP si comporta in modo diverso per le modifiche all'interno e all'esterno della VM. L'ARP non è consigliato per i carichi di lavoro con file ad entropia elevata all'interno della VM.

Modifiche esterne alla macchina virtuale

ARP può rilevare le modifiche all'estensione di un file su un volume NFS esterno alla VM se una nuova estensione entra nel volume crittografato o se cambia l'estensione di un file. Le modifiche all'estensione dei file rilevabili sono:

- vmx
- .vmxf
- .vmdk
- -flat.vmdk
- .nvram
- .vmem
- .vmsd
- .vmsn
- .vswp
- .vmss
- log
- -\#.log

Modifiche all'interno della VM

Se l'attacco ransomware riguarda la macchina virtuale e i file all'interno della macchina virtuale vengono alterati senza apportare modifiche all'esterno della macchina virtuale, ARP rileva la minaccia se l'entropia predefinita della macchina virtuale è bassa (ad esempio file .txt, .docx o .mp4). Anche se ARP crea un'istantanea di protezione in questo scenario, non genera un avviso di minaccia perché le estensioni di file esterne alla VM non sono state manomesse.

Se, per impostazione predefinita, i file sono ad entropia elevata (ad esempio file .gzip o protetti da password), le funzionalità di rilevamento di ARP sono limitate. In questo caso, ARP può ancora acquisire istantanee proattive, tuttavia non verrà attivato alcun avviso se le estensioni dei file non sono state manomesse esternamente.

Configurazioni non supportate

ARP non è supportato nelle seguenti configurazioni di sistema:

- Ambienti ONTAP S3
- Ambienti SAN

ARP non supporta le seguenti configurazioni di volume:

- Volumi FlexGroup (in ONTAP da 9.10.1 a 9.12.1. A partire da ONTAP 9.13.1, sono supportati i volumi FlexGroup)
- FlexCache Volumes (ARP supportato sui volumi FlexVol di origine ma non sui volumi cache)
- Volumi offline
- Volumi solo SAN
- Volumi SnapLock
- SnapMirror sincrono
- SnapMirror asincrono (non supportato solo in ONTAP 9.10.1 e 9.11.1. SnapMirror asincrono è supportato a partire da ONTAP 9.12.1. Per ulteriori informazioni, vedere [snapmirror].)
- Volumi limitati
- Volumi root di storage VM
- Volumi di VM storage interrotte

Considerazioni sulle performance e sulla frequenza ARP

ARP può avere un impatto minimo sulle prestazioni del sistema, misurato in termini di throughput e IOPS di picco. L'impatto della funzionalità ARP dipende dai carichi di lavoro dei volumi specifici. Per i carichi di lavoro comuni, si consigliano i seguenti limiti di configurazione:

Caratteristiche del carico di lavoro	Limite di volume consigliato per nodo	Peggioramento delle performance con superamento del limite di volume per nodo:[*]
I dati possono essere compressi o a uso intensivo di lettura.	150	4% degli IOPS massimi
I dati non possono essere compressi con un utilizzo intensivo di scrittura.	60	10% degli IOPS massimi

Superato:[*] le performance di sistema non vengono degradate oltre queste percentuali, indipendentemente dal numero di volumi aggiunti in eccesso rispetto ai limiti raccomandati.

Poiché gli analytics ARP vengono eseguiti in una sequenza con priorità, con l'aumentare del numero di volumi protetti, gli analytics vengono eseguiti su ciascun volume con minore frequenza.

Verifica multi-admin con volumi protetti con ARP

A partire da ONTAP 9.13.1, è possibile attivare la verifica multi-admin (MAV) per una maggiore sicurezza con ARP. MAV garantisce che almeno due o più amministratori autenticati siano tenuti a disattivare ARP, sospendere ARP o contrassegnare un attacco sospetto come falso positivo su un volume protetto. Scopri come "Abilitare MAV per volumi protetti da ARP".

È necessario definire gli amministratori per un gruppo MAV e creare regole MAV per `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, e. `security anti-ransomware volume attack clear-suspect` Comandi ARP che si desidera proteggere. Ogni amministratore del gruppo MAV deve approvare ogni nuova richiesta di regola e. "Aggiungere nuovamente la regola MAV" Nelle impostazioni MAV.

A partire da ONTAP 9.14.1, ARP offre avvisi per la creazione di un'istantanea ARP e per l'osservazione di una

nuova estensione di file. Gli avvisi per questi eventi sono disattivati per impostazione predefinita. Gli avvisi possono essere impostati a livello di volume o SVM. È possibile creare regole MAV a livello SVM utilizzando `security anti-ransomware vserver event-log modify` o al livello del volume con `security anti-ransomware volume event-log modify`.

Passi successivi

- "Attiva la protezione ransomware autonoma"
- "Abilita MAV per volumi protetti da ARP"

Attiva la protezione ransomware autonoma

A partire da ONTAP 9.10.1, è possibile attivare la protezione ransomware autonoma (ARP) su volumi nuovi o esistenti. Per prima cosa, si attiva ARP in modalità di apprendimento, in cui il sistema analizza il carico di lavoro per caratterizzare il comportamento normale. È possibile attivare ARP su un volume esistente oppure creare un nuovo volume e attivare ARP dall'inizio.

A proposito di questa attività

Si dovrebbe sempre abilitare ARP inizialmente in modalità di apprendimento (o dry-run). L'avvio in modalità attiva può causare un numero eccessivo di falsi positivi.

Si consiglia di far funzionare ARP in modalità di apprendimento per un minimo di 30 giorni. A partire da ONTAP 9.13.1, ARP determina automaticamente l'intervallo ottimale del periodo di apprendimento e automatizza lo switch, che può verificarsi prima di 30 giorni. Per ulteriori informazioni, vedere "Modalità di apprendimento e attive".

> Nei volumi esistenti, l'apprendimento e le modalità attive si applicano solo ai dati scritti di recente, non ai dati già esistenti nel volume. I dati esistenti non vengono sottoposti a scansione e analizzati, poiché le caratteristiche del traffico dati normale precedente vengono assunte in base ai nuovi dati dopo che il volume è stato abilitato per ARP.

Prima di iniziare

- Devi avere una macchina virtuale per lo storage (SVM) abilitata per NFS o SMB (o entrambi).
- Il licenza corretta Deve essere installato per la versione di ONTAP in uso.
- È necessario disporre di un carico di lavoro NAS con i client configurati.
- Il volume che si desidera impostare ARP deve essere protetto e deve avere un attivo "percorso di giunzione".
- Il volume deve essere pieno al di sotto del 100%.
- Si consiglia di configurare il sistema EMS per l'invio di notifiche e-mail, che includano avvisi relativi all'attività ARP. Per ulteriori informazioni, vedere "Configurare gli eventi EMS per l'invio di notifiche e-mail".
- A partire da ONTAP 9.13.1, si consiglia di attivare la verifica multi-admin (MAV) in modo che siano necessari due o più amministratori utente autenticati per la configurazione ARP (Autonomous ransomware Protection). Per ulteriori informazioni, vedere "Attiva la verifica multi-admin".

Enable ARP (attiva ARP)

È possibile attivare ARP utilizzando Gestione di sistema o l'interfaccia CLI di ONTAP.

System Manager

Fasi

1. Selezionare **Storage > Volumes** (archiviazione > volumi), quindi selezionare il volume che si desidera proteggere.
2. Nella scheda **Security** della panoramica **Volumes**, selezionare **Status** per passare da Disabled (Disattivato) a Enabled (attivato) in Learning-mode (modalità apprendimento) nella casella **Anti-ransomware**.
3. Al termine del periodo di apprendimento, impostare ARP in modalità attiva.

   > A partire da ONTAP 9.13.1, ARP determina automaticamente l'intervallo ottimale del periodo di apprendimento e automatizza lo switch. È possibile "Disattivare questa impostazione sulla VM di storage associata" se si desidera controllare manualmente la modalità di apprendimento in modalità attiva, passare alla modalità attiva.

   a. Selezionare **Storage > Volumes** (archiviazione > volumi), quindi selezionare il volume pronto per la modalità attiva.
   b. Nella scheda **Security** della panoramica **Volumes**, selezionare **Switch** to Active mode nella casella Anti-ransomware.
4. È possibile verificare lo stato ARP del volume nella casella **Anti-ransomware**.

   Per visualizzare lo stato ARP per tutti i volumi: Nel riquadro **Volumes** (volumi), selezionare **Show/Hide** (Mostra/Nascondi), quindi assicurarsi che sia selezionato lo stato **Anti-ransomware**.

CLI

Il processo di abilitazione dell'ARP con la CLI differisce se lo si attiva su un volume esistente rispetto a un nuovo volume.

Attivare ARP su un volume esistente

1. Modificare un volume esistente per abilitare la protezione ransomware in modalità di apprendimento:

   ```
   security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
   ```

   Se si esegue ONTAP 9.13.1 o versione successiva, l'apprendimento adattivo viene attivato in modo che il passaggio allo stato attivo venga eseguito automaticamente. Se non si desidera che questo comportamento venga attivato automaticamente, modificare l'impostazione a livello di SVM su tutti i volumi associati:

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

2. Al termine del periodo di apprendimento, modificare il volume protetto per passare alla modalità attiva, se non è già stato eseguito automaticamente:

   ```
   security anti-ransomware volume enable -volume vol_name -vserver svm_name
   ```

   È anche possibile passare alla modalità attiva con il comando modify volume:

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   active
   ```

3. Verificare lo stato ARP del volume.

   ```
   security anti-ransomware volume show
   ```

Abilitare ARP su un nuovo volume

1. Creare un nuovo volume con la protezione anti-ransomware abilitata prima del provisioning dei dati.

   ```
   volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size
   nn -anti-ransomware-state dry-run -junction-path /path_name
   ```

   Se si esegue ONTAP 9.13.1 o versione successiva, l'apprendimento adattivo viene attivato in modo che il passaggio allo stato attivo venga eseguito automaticamente. Se non si desidera che questo comportamento venga attivato automaticamente, modificare l'impostazione a livello di SVM su tutti i volumi associati:

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

2. Al termine del periodo di apprendimento, modificare il volume protetto per passare alla modalità attiva, se non è già stato eseguito automaticamente:

   ```
   security anti-ransomware volume enable -volume vol_name -vserver svm_name
   ```

   È anche possibile passare alla modalità attiva con il comando modify volume:

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   active
   ```

3. Verificare lo stato ARP del volume.

   ```
   security anti-ransomware volume show
   ```

Attiva la protezione ransomware autonoma per impostazione predefinita nei nuovi volumi

A partire da ONTAP 9.10.1, è possibile configurare le VM di storage in modo che i nuovi volumi siano attivati per impostazione predefinita per la protezione ransomware autonoma (ARP) in modalità di apprendimento.

A proposito di questa attività

Per impostazione predefinita, i nuovi volumi vengono creati con ARP in modalità disattivata. È possibile modificare questa impostazione in System Manager e con l'interfaccia CLI. I volumi abilitati per impostazione predefinita sono impostati su ARP in modalità di apprendimento (o dry-run).

ARP viene attivato solo sui volumi creati in SVM dopo aver modificato l'impostazione. ARP non verrà abilitato sui volumi esistenti. Scopri come "Abilitare ARP in un volume esistente".

A partire da ONTAP 9.13.1, l'apprendimento adattivo è stato aggiunto agli analytics ARP e il passaggio dalla modalità di apprendimento alla modalità attiva viene eseguito automaticamente. Per ulteriori informazioni, vedere "Modalità di apprendimento e attive".

Prima di iniziare

- Il licenza corretta Deve essere installato per la versione di ONTAP in uso.
- Il volume deve essere pieno al di sotto del 100%.
- I percorsi di giunzione devono essere attivi.
- A partire da ONTAP 9.13.1, si consiglia di attivare la verifica multi-admin (MAV) in modo che siano necessari due o più amministratori utente autenticati per le operazioni anti-ransomware. "Scopri di più".

Passare dalla modalità di apprendimento alla modalità attiva

A partire da ONTAP 9.13.1, l'apprendimento adattivo è stato aggiunto all'analisi ARP. Il passaggio dalla modalità di apprendimento alla modalità attiva viene eseguito automaticamente. La decisione autonoma di ARP di passare automaticamente dalla modalità di apprendimento alla modalità attiva si basa sulle impostazioni di configurazione delle seguenti opzioni:

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

Dopo 30 giorni di apprendimento, un volume passa automaticamente alla modalità attiva anche se una o più di queste condizioni non sono soddisfatte. In altre parole, se la funzione di commutazione automatica è attivata, il volume passa alla modalità attiva dopo un massimo di 30 giorni. Il valore massimo di 30 giorni è fisso e non modificabile.

Per ulteriori informazioni sulle opzioni di configurazione ARP, compresi i valori predefiniti, consultare la "Riferimento al comando ONTAP".

Fasi

È possibile utilizzare Gestione di sistema o la CLI di ONTAP per attivare ARP per impostazione predefinita.

System Manager

1. Selezionare **Storage > Storage VM** (Storage VM > Storage VM), quindi selezionare la VM di storage contenente i volumi che si desidera proteggere con ARP.
2. Selezionare la scheda **Impostazioni**. In **sicurezza**, individuare il riquadro **Anti-ransomware**, quindi selezionare
3. Selezionare la casella per abilitare ARP per volumi NAS. Selezionare la casella aggiuntiva per abilitare ARP su tutti i volumi NAS idonei nella VM di storage.

> Se è stato eseguito l'aggiornamento a ONTAP 9.13.1, l'impostazione **passa automaticamente dalla modalità di apprendimento alla modalità attiva dopo un apprendimento sufficiente** viene attivata automaticamente. Ciò consente ad ARP di determinare l'intervallo ottimale del periodo di apprendimento e di automatizzare il passaggio alla modalità attiva. Disattivare l'impostazione se si desidera passare manualmente alla modalità attiva.

CLI

1. Modificare una SVM esistente per attivare ARP per impostazione predefinita nei nuovi volumi:
   `vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run`

   Nella CLI, è anche possibile creare una nuova SVM con ARP attivato per impostazione predefinita per i nuovi volumi.
   `vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]`

   Se è stato eseguito l'aggiornamento a ONTAP 9.13.1 o versioni successive, l'apprendimento adattivo viene attivato in modo che il passaggio allo stato attivo venga eseguito automaticamente. Se non si desidera attivare automaticamente questo comportamento, utilizzare il seguente comando:

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

Sospendere la protezione ransomware autonoma per escludere gli eventi dei workload dall'analisi

Se si prevedono eventi insoliti relativi ai carichi di lavoro, è possibile sospendere temporaneamente e riprendere l'analisi ARP (Autonomous ransomware Protection) in qualsiasi momento.

A partire da ONTAP 9.13.1, è possibile attivare la verifica multi-admin (MAV) in modo che due o più amministratori utente autenticati siano necessari per mettere in pausa l'ARP. "Scopri di più".

A proposito di questa attività

Durante una pausa ARP, non vengono registrati eventi né vengono eseguite azioni per nuove scritture. Tuttavia, l'operazione di analisi continua per i log precedenti in background.

Non utilizzare la funzione di disattivazione ARP per mettere in pausa gli analytics. In questo modo si disattiva l'ARP sul volume e tutte le informazioni esistenti sul comportamento dei carichi di lavoro appresi vengono perse. Ciò richiederebbe un riavvio del periodo di apprendimento.

Fasi

È possibile utilizzare Gestione di sistema o la CLI di ONTAP per sospendere ARP.

System Manager

1. Selezionare **Storage > Volumes** (archiviazione > volumi*), quindi selezionare il volume in cui si desidera sospendere l'ARP.
2. Nella scheda **sicurezza** della panoramica dei volumi, seleziona **Pausa anti-ransomware** nella casella **Anti-ransomware**.

> A partire da ONTAP 9.13.1, se si utilizza MAV per proteggere le impostazioni ARP, l'operazione di pausa richiede di ottenere l'approvazione di uno o più amministratori aggiuntivi. "L'approvazione deve essere ricevuta da tutti gli amministratori" Associato al gruppo di approvazione MAV o l'operazione non riuscirà.

CLI

1. Pausa ARP su un volume:

   ```
   security anti-ransomware volume pause -vserver svm_name -volume vol_name
   ```

2. Per riprendere l'elaborazione, utilizzare `resume` parametro.

   ```
   security anti-ransomware volume resume -vserver svm_name -volume vol_name
   ```

3. **Se si utilizza MAV (disponibile con ARP che inizia con ONTAP 9.13.1) per proteggere le impostazioni ARP,** l'operazione di pausa richiede l'approvazione di uno o più amministratori aggiuntivi. L'approvazione deve essere ricevuta da tutti gli amministratori associati al gruppo di approvazione MAV, altrimenti l'operazione non avrà esito positivo.

   Se si utilizza MAV e un'operazione di pausa prevista richiede ulteriori approvazioni, ciascun responsabile dell'approvazione del gruppo MAV esegue le seguenti operazioni:

   a. Mostra la richiesta:

      ```
      security multi-admin-verify request show
      ```

   b. Approvare la richiesta:

      ```
      security multi-admin-verify request approve -index[number returned from show request]
      ```

      La risposta dell'ultimo responsabile dell'approvazione del gruppo indica che il volume è stato modificato e che lo stato di ARP è in pausa.

      Se si utilizza MAV e si è un responsabile dell'approvazione del gruppo MAV, è possibile rifiutare una richiesta di operazione di pausa:

   ```
   security multi-admin-verify request veto -index[number returned from show request]
   ```

Gestire i parametri di rilevamento degli attacchi tramite protezione autonoma dal ransomware

A partire da ONTAP 9.11.1, puoi modificare i parametri per il rilevamento del ransomware su un volume abilitato alla protezione autonoma contro il ransomware specifico e segnalare un picco noto come normale attività dei file. La regolazione dei parametri di rilevamento consente di migliorare l'accuratezza dei rapporti in base al carico di lavoro del volume specifico.

Come funziona il rilevamento degli attacchi

Quando la protezione autonoma da ransomware (ARP) è in modalità di apprendimento, sviluppa valori di base per i comportamenti di volume. Si tratta di entropia, estensioni dei file e, a partire da ONTAP 9.11.1, IOPS. Queste baseline vengono utilizzate per valutare le minacce ransomware. Per ulteriori informazioni su questi criteri, vedere Cosa rileva ARP.

In ONTAP 9.10.1, ARP genera un avviso se rileva entrambe le seguenti condizioni:

- più di 20 file con estensioni non precedentemente osservate nel volume
- elevati dati di entropia

A partire da ONTAP 9.11.1, ARP emette un avviso di minaccia se *solo* viene soddisfatta una condizione. Ad esempio, se si osservano più di 20 file con estensioni che non sono state precedentemente osservate nel volume entro un periodo di 24 ore, ARP lo classificherà come una minaccia *indipendentemente* dall'entropia osservata. (I valori dei file 24 ore e 20 sono predefiniti, che possono essere modificati).

A partire da ONTAP 9.14.1, è possibile configurare gli avvisi quando ARP osserva una nuova estensione di file e quando ARP crea un'istantanea. Per ulteriori informazioni, vedere [modify-alerts]

Alcuni volumi e carichi di lavoro richiedono parametri di rilevamento diversi. Ad esempio, il volume abilitato per ARP può ospitare numerosi tipi di estensioni di file, nel qual caso è possibile modificare il conteggio delle soglie per le estensioni di file mai viste prima a un numero maggiore del valore predefinito di 20 o disattivare gli avvisi in base alle estensioni di file mai viste prima. A partire da ONTAP 9.11.1, puoi modificare i parametri di rilevamento degli attacchi per adattarli meglio ai tuoi carichi di lavoro specifici.

Modificare i parametri di rilevamento degli attacchi

A seconda dei comportamenti previsti del volume abilitato per ARP, è possibile modificare i parametri di rilevamento degli attacchi.

Fasi

1. Visualizzare i parametri di rilevamento degli attacchi esistenti:

   ```
   security anti-ransomware volume attack-detection-parameters show -vserver
   svm_name -volume volume_name
   ```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
                                          Vserver Name : vs1
                                           Volume Name : vol1
            Is Detection Based on High Entropy Data Rate? : true
  Is Detection Based on Never Seen before File Extension? : true
                 Is Detection Based on File Create Rate? : true
                 Is Detection Based on File Rename Rate? : true
                 Is Detection Based on File Delete Rate? : true
           Is Detection Relaxing Popular File Extensions? : true
                High Entropy Data Surge Notify Percentage : 100
                 File Create Rate Surge Notify Percentage : 100
                 File Rename Rate Surge Notify Percentage : 100
                 File Delete Rate Surge Notify Percentage : 100
 Never Seen before File Extensions Count Notify Threshold : 20
       Never Seen before File Extensions Duration in Hour : 24
```

2. Tutti i campi visualizzati sono modificabili con valori booleani o interi. Per modificare un campo, utilizzare `security anti-ransomware volume attack-detection-parameters modify` comando.

   Per un elenco completo dei parametri, vedere "Riferimento al comando ONTAP".

Segnalare le sovratensioni note

ARP continua a modificare i valori di base per i parametri di rilevamento anche in modalità attiva. Se conoscete i picchi nella vostra attività di volume—o un aumento una volta o un aumento che è caratteristica di una nuova normale—dovreste segnalarlo come sicuro. La segnalazione manuale di questi picchi come sicuri aiuta a migliorare l'accuratezza delle valutazioni delle minacce di ARP.

Segnalare un aumento di una tantum

1. Se in circostanze note si verifica un picco una tantum e si desidera che ARP segnali un aumento simile in circostanze future, eliminare il picco dal comportamento del carico di lavoro:

   ```
   security anti-ransomware volume workload-behavior clear-surge -vserver
   svm_name -volume volume_name
   ```

Modificare il picco della linea di base

1. Se un picco segnalato deve essere considerato un normale comportamento dell'applicazione, riportare il picco in quanto tale per modificare il valore di picco della linea di base.

   ```
   security anti-ransomware volume workload-behavior update-baseline-from-surge
   -vserver svm_name -volume volume_name
   ```

Configurare gli avvisi ARP

A partire da ONTAP 9.14.1, ARP consente di specificare gli avvisi per due eventi ARP:

- Osservazione della nuova estensione di un file su un volume

- Creazione di un’istantanea ARP

È possibile impostare avvisi per questi due eventi su singoli volumi o per l’intera SVM. Se abiliti gli avvisi per la SVM, le impostazioni degli avvisi vengono ereditate solo dai volumi creati in seguito all’attivazione della funzione di avviso. Per impostazione predefinita, gli avvisi non sono attivati su alcun volume.

Gli avvisi di eventi possono essere controllati con verifica multi-admin. Per ulteriori informazioni, vedere Verifica multi-admin con volumi protetti con ARP.

System Manager

Impostare gli avvisi per un volume

1. Passare a **volumi**. Selezionare il singolo volume per il quale si desidera modificare le impostazioni.
2. Selezionare la scheda **sicurezza**, quindi **Impostazioni protezione eventi**.
3. Per ricevere avvisi relativi a **Nuova estensione rilevata** e **istantanea ransomware creata**, selezionare il menu a discesa sotto l'intestazione **gravità**. Modificare l'impostazione da **non generare evento** a **Avviso**.
4. Selezionare **Salva**.

Impostare gli avvisi per una SVM

1. Accedere a **Storage VM** quindi selezionare la SVM per la quale si desidera abilitare le impostazioni.
2. Sotto l'intestazione **sicurezza**, individuare la scheda **Anti-ransomware**. Selezionare ⋮ Quindi **Modifica gravità evento ransomware**.
3. Per ricevere avvisi relativi a **Nuova estensione rilevata** e **istantanea ransomware creata**, selezionare il menu a discesa sotto l'intestazione **gravità**. Modificare l'impostazione da **non generare evento** a **Avviso**.
4. Selezionare **Salva**.

CLI

Impostare gli avvisi per un volume

- Per impostare gli avvisi per una nuova estensione file:

  ```
  security anti-ransomware volume event-log modify -vserver svm_name -is
  -enabled-on-new-file-extension-seen true
  ```

- Per impostare gli avvisi per la creazione di un'istantanea ARP:

  ```
  security anti-ransomware volume event-log modify -vserver svm_name -is
  -enabled-on-snapshot-copy-creation true
  ```

- Confermare le impostazioni con `anti-ransomware volume event-log show` comando.

Impostare gli avvisi per una SVM

- Per impostare gli avvisi per una nuova estensione file:

  ```
  security anti-ransomware vserver event-log modify -vserver svm_name -is
  -enabled-on-new-file-extension-seen true
  ```

- Per impostare gli avvisi per la creazione di un'istantanea ARP:

  ```
  security anti-ransomware vserver event-log modify -vserver svm_name -is
  -enabled-on-snapshot-copy-creation true
  ```

- Confermare le impostazioni con `security anti-ransomware vserver event-log show` comando.

Ulteriori informazioni

- "Comprendere gli attacchi di protezione autonoma da ransomware e lo snapshot di protezione autonoma da ransomware"

Rispondere ad attività anomale

Quando la protezione ransomware autonoma (ARP) rileva attività anomale in un volume protetto, emette un avviso. È necessario valutare la notifica per determinare se l'attività è accettabile (falso positivo) o se un attacco sembra dannoso.

A proposito di questa attività

ARP visualizza un elenco di file sospetti quando rileva una combinazione di elevata entropia dei dati, attività anomale del volume con crittografia dei dati e estensioni di file insolite.

Quando viene visualizzato l'avviso, è possibile rispondere contrassegnando l'attività del file in uno dei due modi seguenti:

- **Falso positivo**

  Il tipo di file identificato è previsto nel carico di lavoro e può essere ignorato.

- **Potenziale attacco ransomware**

  Il tipo di file identificato non è previsto nel carico di lavoro e deve essere trattato come un potenziale attacco.

In entrambi i casi, il normale monitoraggio riprende dopo l'aggiornamento e la cancellazione degli avvisi. ARP registra la valutazione nel profilo di valutazione delle minacce, utilizzando la scelta dell'utente per monitorare le attività successive dei file.

In caso di attacco sospetto, è necessario determinare se si tratta di un attacco, rispondere al caso in cui si tratti e ripristinare i dati protetti prima di cancellare le notifiche. "Scopri di più su come eseguire il ripristino da un attacco ransomware".

> Se si ripristina un intero volume, non vi sono avvisi da cancellare.

Prima di iniziare

ARP deve essere in esecuzione in modalità attiva.

Fasi

È possibile utilizzare Gestione sistema o l'interfaccia CLI di ONTAP per rispondere a un'attività anomala.

System Manager

1. Quando si riceve una notifica di "attività anomala", seguire il collegamento o passare alla scheda **sicurezza** della panoramica **volumi**.

   Gli avvisi vengono visualizzati nel riquadro **Panoramica** del menu **Eventi**.

2. Quando viene visualizzato il messaggio "rilevata attività anomala del volume", visualizzare i file sospetti.

   Nella scheda **protezione**, selezionare **Visualizza tipi di file sospetti**.

3. Nella finestra di dialogo **tipi di file sospetti**, esaminare ciascun tipo di file e contrassegnarlo come "falso positivo" o "potenziale attacco ransomware".

Se si seleziona questo valore…	Eseguire questa azione…
Falso positivo	Selezionare **Aggiorna** e **Cancella tipi di file sospetti** per registrare la decisione e riprendere il normale monitoraggio ARP. A partire da ONTAP 9.13.1, se si utilizza MAV per proteggere le impostazioni ARP, l'operazione che si sospetta venga richiesta l'approvazione di uno o più amministratori aggiuntivi. "L'approvazione deve essere ricevuta da tutti gli amministratori" Associato al gruppo di approvazione MAV o l'operazione non riuscirà.
Potenziale attacco ransomware	Rispondere all'attacco e ripristinare i dati protetti. Quindi selezionare **Aggiorna** e **Cancella tipi di file sospetti** per registrare la decisione e riprendere il normale monitoraggio ARP. Non esistono tipi di file sospetti da eliminare se è stato ripristinato un intero volume.

CLI

1. Quando ricevi una notifica di un attacco ransomware sospetto, verifica l'ora e la gravità dell'attacco:

   ```
   security anti-ransomware volume show -vserver svm_name -volume vol_name
   ```

   Output di esempio:

   ```
   Vserver Name: vs0
   Volume Name: vol1
   State: enabled
   Attack Probability: moderate
   Attack Timeline: 9/14/2021 01:03:23
   Number of Attacks: 1
   ```

   È inoltre possibile controllare i messaggi EMS:

```
event log show -message-name callhome.arw.activity.seen
```

2. Generare un report sugli attacchi e prendere nota della posizione di output:

   ```
   security anti-ransomware volume attack generate-report -volume vol_name
   -dest-path file_location/
   ```

   Output di esempio:

   ```
   Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
   "vs0:vol1/"
   ```

3. Visualizzare il report su un sistema client di amministrazione. Ad esempio:

   ```
   [root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08

   19  "9/14/2021 01:03:23"   test_dir_1/test_file_1.jpg.lckd
   20  "9/14/2021 01:03:46"   test_dir_2/test_file_2.jpg.lckd
   21  "9/14/2021 01:03:46"   test_dir_3/test_file_3.png.lckd`
   ```

4. Eseguire una delle seguenti operazioni in base alla valutazione delle estensioni dei file:

   - Falso positivo

     Immettere il seguente comando per registrare la decisione, aggiungere il nuovo interno all'elenco di quelli consentiti e riprendere il normale monitoraggio anti-ransomware:
     `anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true`

     Per identificare gli interni, utilizzare uno dei seguenti parametri:
     `[-seq-no integer]` Numero di sequenza del file nell'elenco dei file sospetti.
     `[-extension text, … ]` Estensioni di file
     `[-start-time date_time -end-time date_time]` Orari di inizio e fine dell'intervallo di file da cancellare, nel formato "MM/GG/AAAA HH:MM:SS".

   - Potenziale attacco ransomware

     Rispondere all'attacco e. "Recuperare i dati dallo snapshot di backup creato da ARP". Una volta ripristinati i dati, immettere il seguente comando per registrare la decisione e riprendere il normale monitoraggio ARP:

     `anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive false`

     Per identificare gli interni, utilizzare uno dei seguenti parametri:
     `[-seq-no integer]` Numero di sequenza del file nell'elenco dei file sospetti
     `[-extension text, … ]` Estensione del file
     `[-start-time date_time -end-time date_time]` Orari di inizio e fine dell'intervallo di file da cancellare, nel formato "MM/GG/AAAA HH:MM:SS".

Non esistono tipi di file sospetti da eliminare se è stato ripristinato un intero volume. Lo snapshot di backup creato da ARP verrà rimosso e il report dell'attacco verrà cancellato.

5. Se si sta utilizzando MAV e un previsto `clear-suspect` L'operazione richiede approvazioni aggiuntive, ogni responsabile dell'approvazione del gruppo MAV esegue le seguenti operazioni:

   a. Mostra la richiesta:

   ```
   security multi-admin-verify request show
   ```

   b. Approvare la richiesta di riprendere il normale monitoraggio anti-ransomware:

   ```
   security multi-admin-verify request approve -index[number returned from show request]
   ```

   La risposta dell'ultimo responsabile dell'approvazione del gruppo indica che il volume è stato modificato e che viene registrato un falso positivo.

6. Se si utilizza MAV e si è un responsabile dell'approvazione del gruppo MAV, è anche possibile rifiutare una richiesta con un sospetto chiaro:

   ```
   security multi-admin-verify request veto -index[number returned from show request]
   ```

Ulteriori informazioni

- "KB: Comprendere gli attacchi di protezione ransomware autonoma e lo snapshot di protezione ransomware autonoma".

Ripristinare i dati dopo un attacco ransomware

La protezione autonoma dal ransomware (ARP) crea copie Snapshot denominate `Anti_ransomware_backup` quando rileva una potenziale minaccia ransomware. È possibile utilizzare una di queste copie snapshot ARP o un'altra copia Snapshot del volume per ripristinare i dati.

A proposito di questa attività

Se il volume presenta relazioni SnapMirror, replicare manualmente tutte le copie mirror del volume immediatamente dopo il ripristino da una copia Snapshot. In caso contrario, le copie mirror non possono essere utilizzabili e devono essere eliminate e ricreate.

Per eseguire il ripristino da uno Snapshot diverso da `Anti_ransomware_backup` Snapshot dopo aver identificato un attacco di sistema, è necessario prima rilasciare lo snapshot ARP.

Se non è stato segnalato alcun attacco al sistema, è necessario prima eseguire il ripristino da `Anti_ransomware_backup` La copia Snapshot, quindi, completa un successivo ripristino del volume dalla copia Snapshot scelta.

Fasi

Per ripristinare i dati, è possibile utilizzare Gestione di sistema o l'interfaccia utente di ONTAP.

System Manager

Ripristino dopo un attacco di sistema

1. Per eseguire il ripristino dall'istantanea ARP, passare direttamente al punto 2. Per eseguire il ripristino da una copia Snapshot precedente, è necessario prima rilasciare il blocco sull'istantanea ARP.
   a. Selezionare **Storage > Volumes** (Storage > volumi).
   b. Selezionare **sicurezza**, quindi **Visualizza tipi di file sospetti**
   c. Contrassegnare i file come "False Positive" (Falso positivo).
   d. Selezionare **Aggiorna** e **Cancella tipi di file sospetti**
2. Visualizzare le copie Snapshot nei volumi:

   Selezionare **archiviazione > volumi**, quindi selezionare il volume e **Snapshot Copies**.

3. Selezionare ⋮ Accanto alla copia istantanea che si desidera ripristinare, quindi **Restore**.

Ripristinare se non è stato identificato un attacco di sistema

1. Visualizzare le copie Snapshot nei volumi:

   Selezionare **archiviazione > volumi**, quindi selezionare il volume e **Snapshot Copies**.

2. Selezionare ⋮ loro scelgono il `Anti_ransomware_backup` Istantanea.
3. Selezionare **Restore** (Ripristina).
4. Tornare al menu **Snapshot Copies**, quindi scegliere la copia istantanea che si desidera utilizzare. Selezionare **Restore** (Ripristina).

CLI

Ripristino dopo un attacco di sistema

1. Per eseguire il ripristino dalla copia snapshot ARP, passare direttamente al punto 2. Per ripristinare i dati da copie Snapshot precedenti, è necessario rilasciare il blocco sullo snapshot ARP.

   > È necessario rilasciare il SnapLock anti-ransomware solo prima di eseguire il ripristino dalle copie Snapshot precedenti, se si utilizza `volume snap restore` come descritto di seguito. Se si ripristinano i dati utilizzando Flex Clone, Single file Snap Restore o altri metodi, ciò non è necessario.

   Contrassegnare l'attacco come "falso positivo" e "chiaro sospetto":
   `anti-ransomware volume attack clear-suspect -vserver` *`svm_name`* `-volume` *`vol_name`* `[`*`extension identifiers`*`] -false-positive true`
   Per identificare gli interni, utilizzare uno dei seguenti parametri:
   `[-seq-no` *`integer`*`]` Numero di sequenza del file nell'elenco dei file sospetti.
   `[-extension` *`text`*`, … ]` Estensioni di file
   `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` Orari di inizio e fine dell'intervallo di file da cancellare, nel formato "MM/GG/AAAA HH:MM:SS".

2. Elencare le copie Snapshot in un volume:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   L'esempio seguente mostra le copie Snapshot in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

3. Ripristinare il contenuto di un volume da una copia Snapshot:

   `volume snapshot restore -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`*

   Nell'esempio riportato di seguito viene ripristinato il contenuto di `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

Ripristinare se non è stato identificato un attacco di sistema

1. Elencare le copie Snapshot in un volume:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   L'esempio seguente mostra le copie Snapshot in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Ripristinare il contenuto di un volume da una copia Snapshot:

   `volume snapshot restore -vserver SVM -volume volume -snapshot snapshot`

   Nell'esempio riportato di seguito viene ripristinato il contenuto di `vol1`:

   ```
   cluster1::> volume snapshot restore -vserver vs0 -volume vol1
   -snapshot daily.2013-01-25_0010
   ```

3. Ripetere i passaggi 1 e 2 per ripristinare il volume utilizzando la copia Snapshot desiderata.

Ulteriori informazioni

- "KB: Prevenzione e recovery dal ransomware in ONTAP"

Modificare le opzioni per le copie Snapshot automatiche

A partire da ONTAP 9.11.1, puoi utilizzare la CLI per controllare le impostazioni di conservazione per le copie Snapshot di protezione autonoma dal ransomware (ARP), generate automaticamente in risposta a sospetti attacchi ransomware.

Prima di iniziare

È possibile modificare solo le opzioni di ARP Snapshot su una SVM di nodo.

Fasi

1. Per visualizzare tutte le impostazioni di copia correnti di ARP Snapshot, immettere:
   `vserver options -vserver svm_name arw*`

   > Il `vserver options` command è un comando nascosto. Per visualizzare la pagina man, immettere `man vserver options` Nella CLI di ONTAP.

2. Per visualizzare le impostazioni di copia correnti di ARP Snapshot, immettere:
   `vserver options -vserver svm_name -option-name arw_setting_name`
3. Per modificare le impostazioni di copia di ARP Snapshot, immettere:
   `vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value`

   È possibile modificare le seguenti impostazioni:

Impostazione ARW	Descrizione
arw.snap.max.count	Specifica il numero massimo di copie Snapshot ARP che possono esistere in un volume in qualsiasi momento. Le copie meno recenti vengono eliminate per garantire che il numero totale di copie Snapshot ARP rientri nel limite specificato.
arw.snap.create.interval.hours	Specifica l'intervallo *in ore* tra le copie snapshot ARP. Una nuova copia Snapshot viene creata quando si sospetta un attacco e la copia creata in precedenza è precedente all'intervallo specificato.

Impostazione ARW	Descrizione
arw.snap.normal.retain.interval.hours	Specifica la durata *in ore* per la quale viene conservata una copia snapshot ARP. Quando una copia ARP Snapshot diventa vecchia, qualsiasi altra copia ARP Snapshot creata prima dell'ultima copia per raggiungere questa età viene eliminata. Nessuna copia snapshot ARP può essere precedente a questa durata.
arw.snap.max.retain.interval.days	Specifica la durata massima *in giorni* per la quale è possibile conservare una copia snapshot ARP. Qualsiasi copia ARP Snapshot precedente a questa durata verrà eliminata se non viene segnalato alcun attacco sul volume. + L'intervallo di conservazione massimo per le copie snapshot ARP viene ignorato se viene rilevata una minaccia moderata. La copia snapshot ARP creata in risposta alla minaccia viene conservata fino a quando non si risponde alla minaccia. Contrassegnare una minaccia come falso positivo eliminare le copie snapshot ARP sul volume.
arw.snap.create.interval.hours.post.max.count	Specifica l'intervallo *in ore* tra le copie snapshot ARP quando il volume contiene già il numero massimo di copie snapshot ARP. Una volta raggiunto il numero massimo di copie, una copia snapshot ARP viene eliminata per creare spazio per una nuova copia. È possibile ridurre la velocità di creazione delle nuove copie Snapshot ARP per conservare le copie meno recenti utilizzando questa opzione. Se il volume contiene già il numero massimo di copie Snapshot ARP, questo intervallo specificato in questa opzione viene utilizzato per la successiva creazione della copia Snapshot ARP, invece di arw.snap.create.interval.hours.
arw.surge.snap.interval.days	Specifica l'intervallo *in giorni* tra le copie snapshot di sovracorrente ARP. ONTAP crea una copia snapshot ARP surge quando c'è un aumento del traffico io e l'ultima copia snapshot ARP creata è precedente a questo intervallo specificato. Questa opzione specifica anche il periodo di conservazione *in giorno* per un'istantanea di sovratensione ARP.

Proteggere dai virus

Panoramica della configurazione antivirus

Vscan è una soluzione di scansione antivirus sviluppata da NetApp che consente ai clienti di proteggere i propri dati da virus o altri codici dannosi.

Vscan esegue scansioni virus quando i client accedono ai file tramite SMB. È possibile configurare Vscan per la scansione on-demand o in base a una pianificazione. È possibile interagire con Vscan utilizzando l'interfaccia a riga di comando (CLI) di ONTAP o le API (Application Programming Interface) di ONTAP.

Informazioni correlate

"Soluzioni partner di Vscan"

Informazioni sulla protezione antivirus di NetApp

Informazioni sulla scansione dei virus NetApp

Vscan è una soluzione di scansione antivirus sviluppata da NetApp che consente ai clienti di proteggere i propri dati da virus o altri codici dannosi. Combina il software antivirus fornito dal partner con le funzionalità ONTAP per offrire ai clienti la flessibilità necessaria per gestire la scansione dei file.

Come funziona la scansione virus

I sistemi storage trasferiscono le operazioni di scansione a server esterni che ospitano software antivirus di terze parti.

In base alla modalità di scansione attiva, ONTAP invia richieste di scansione quando i client accedono ai file tramite SMB (on-access) o accedono ai file in posizioni specifiche, in base a una pianificazione o immediatamente (on-demand).

- È possibile utilizzare *on-access scanning* per verificare la presenza di virus quando i client aprono, leggono, rinominano o chiudono i file su SMB. Le operazioni sui file vengono sospese fino a quando il server esterno non riporta lo stato di scansione del file. Se il file è già stato sottoposto a scansione, ONTAP consente l'operazione. In caso contrario, richiede una scansione dal server.

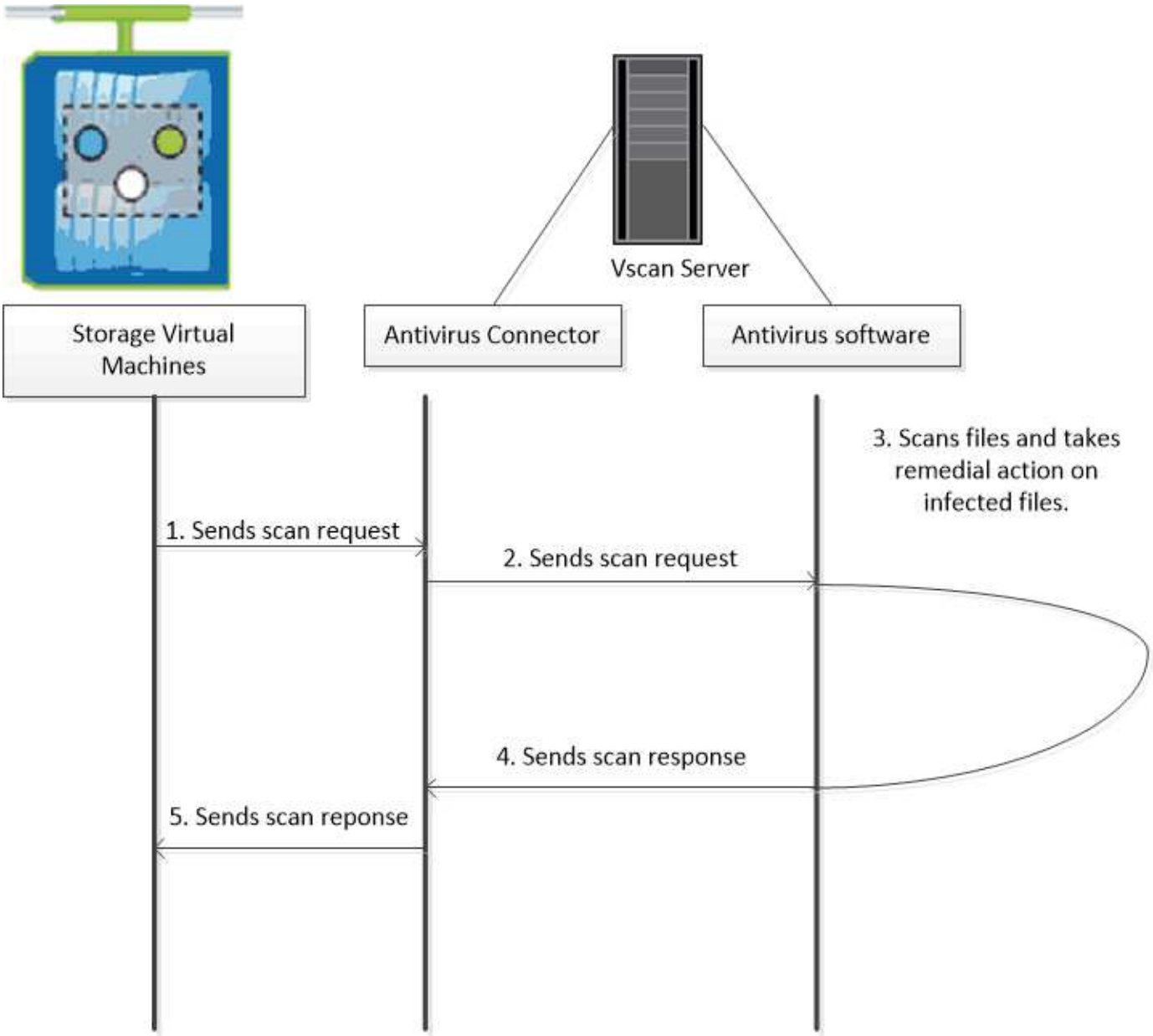
  La scansione on-access non è supportata per NFS.

- È possibile utilizzare la *scansione on-demand* per controllare i file alla ricerca di virus immediatamente o in base a una pianificazione. Si consiglia di eseguire scansioni on-demand solo in ore non di punta per evitare di sovraccaricare l'infrastruttura AV esistente, che è normalmente dimensionata per la scansione on-access. Il server esterno aggiorna lo stato di scansione dei file selezionati, in modo da ridurre la latenza di accesso ai file su SMB. In caso di modifiche al file o aggiornamenti della versione software, viene richiesta una nuova scansione del file dal server esterno.

  È possibile utilizzare la scansione on-demand per qualsiasi percorso nello spazio dei nomi SVM, anche per i volumi esportati solo tramite NFS.

In genere, si abilitano le modalità di scansione on-access e on-demand su una SVM. In entrambe le modalità, il software antivirus esegue un'azione correttiva sui file infetti in base alle impostazioni del software.

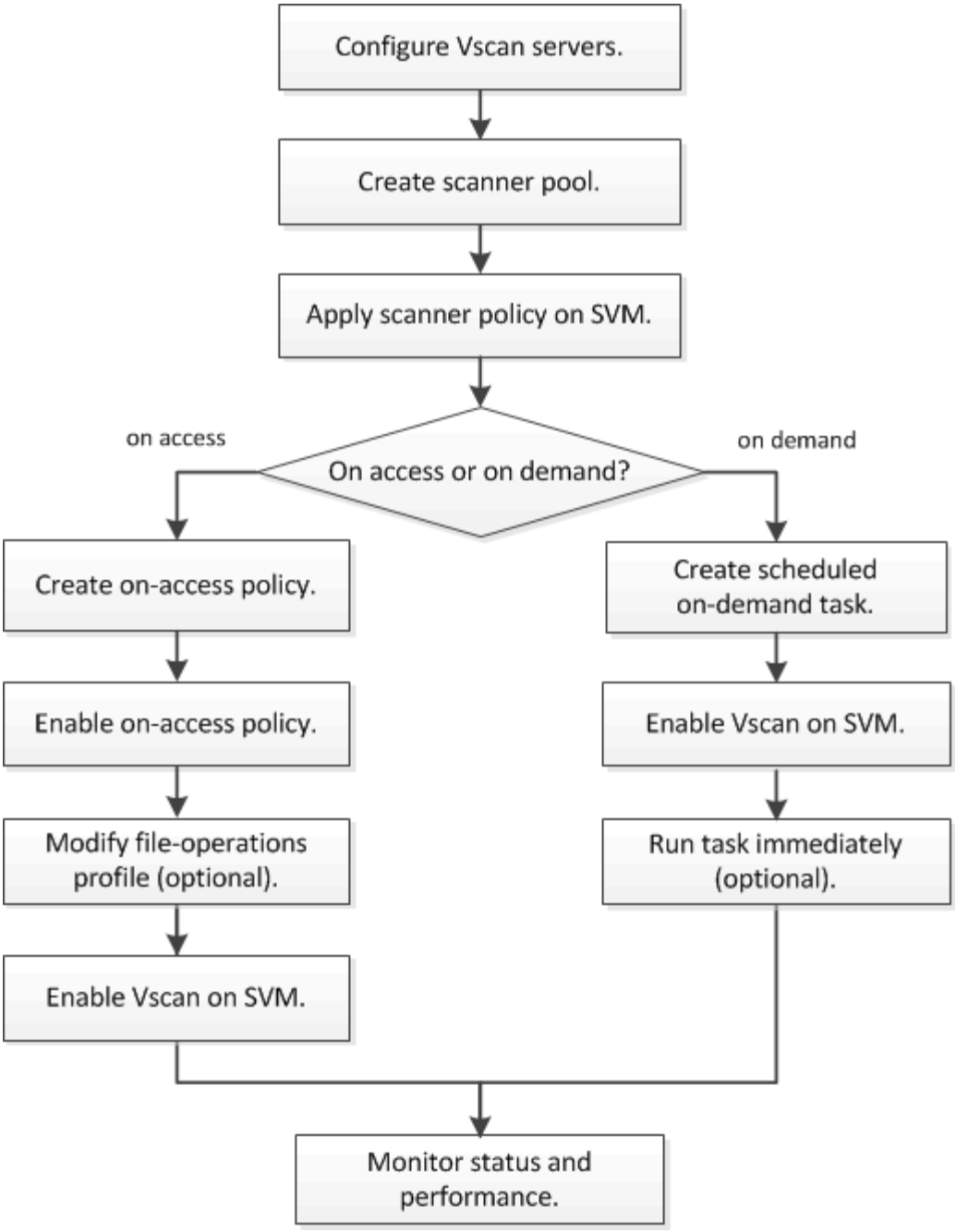
Il connettore antivirus ONTAP, fornito da NetApp e installato sul server esterno, gestisce la comunicazione tra il sistema di storage e il software antivirus.



Workflow di scansione dei virus

Prima di attivare la scansione, è necessario creare un pool di scanner e applicare un criterio scanner. In genere, si abilitano le modalità di scansione on-access e on-demand su una SVM.

È necessario aver completato la configurazione CIFS.



Passi successivi

- Creare un pool di scanner su un singolo cluster
- Applicare un criterio scanner a un singolo cluster
- Creare una policy di accesso

Architettura antivirus

L'architettura antivirus di NetApp è costituita dal software del server Vscan e dalle relative impostazioni.

Software del server Vscan

È necessario installare questo software sul server Vscan.

- **Connettore antivirus ONTAP**

  Si tratta di un software fornito da NetApp che gestisce le comunicazioni di risposta e richiesta di scansione tra le SVM e il software antivirus. Può essere eseguito su una macchina virtuale, ma per ottenere le migliori performance utilizza una macchina fisica. È possibile scaricare questo software dal sito del supporto NetApp (richiede l'accesso).

- **Software antivirus**

  Si tratta di un software fornito dal partner che esegue la scansione dei file alla ricerca di virus o altro codice dannoso. Specificare le azioni correttive da intraprendere sui file infetti durante la configurazione del software.

Impostazioni del software Vscan

È necessario configurare queste impostazioni software sul server Vscan.

- **Scanner pool**

  Questa impostazione definisce i server Vscan e gli utenti con privilegi che possono connettersi alle SVM. Definisce inoltre un periodo di timeout della richiesta di scansione, trascorso il quale la richiesta di scansione viene inviata a un server Vscan alternativo, se disponibile.

  > Impostare il periodo di timeout nel software antivirus sul server Vscan su un valore inferiore di cinque secondi rispetto al periodo di timeout della richiesta di scansione del pool di scanner. In questo modo si evitano situazioni in cui l'accesso al file viene ritardato o negato del tutto perché il periodo di timeout sul software è superiore al periodo di timeout per la richiesta di scansione.

- **Utente con privilegi**

  Questa impostazione è un account utente di dominio utilizzato da un server Vscan per connettersi a SVM. L'account deve essere presente nell'elenco degli utenti con privilegi nel pool di scanner.

- **Criterio scanner**

  Questa impostazione determina se un pool di scanner è attivo. I criteri dello scanner sono definiti dal sistema, pertanto non è possibile creare policy personalizzate dello scanner. Sono disponibili solo queste tre policy:

  - `Primary` specifica che il pool di scanner è attivo.
  - `Secondary` Specifica che il pool di scanner è attivo, solo quando nessuno dei server Vscan nel pool di scanner primario è connesso.
  - `Idle` specifica che il pool di scanner non è attivo.

- **Policy di accesso**

  Questa impostazione definisce l'ambito di una scansione all'accesso. È possibile specificare le dimensioni massime dei file da sottoporre a scansione, le estensioni e i percorsi dei file da includere nella scansione e le estensioni e i percorsi dei file da escludere dalla scansione.

  Per impostazione predefinita, viene eseguita la scansione solo dei volumi di lettura/scrittura. È possibile specificare i filtri che consentono la scansione di volumi di sola lettura o che limitano la scansione ai file aperti con accesso di esecuzione:

- `scan-ro-volume` consente la scansione di volumi di sola lettura.
- `scan-execute-access` limita la scansione ai file aperti con accesso di esecuzione.

> “Execute access” è diverso da “Execute permission”. Un determinato client avrà “Execute Access” su un file eseguibile solo se il file è stato aperto con “Execute Intent”.

È possibile impostare `scan-mandatory` Selezionare Off per specificare che l’accesso al file è consentito quando non sono disponibili server Vscan per la scansione dei virus. Nella modalità on-access è possibile scegliere tra queste due opzioni che si escludono a vicenda:

- Obbligatorio: Con questa opzione, Vscan tenta di inviare la richiesta di scansione al server fino alla scadenza del periodo di timeout. Se la richiesta di scansione non viene accettata dal server, la richiesta di accesso client viene negata.
- Non obbligatorio: Con questa opzione, Vscan consente sempre l’accesso al client, indipendentemente dal fatto che sia disponibile un server Vscan per la scansione dei virus.

- **Attività on-demand**

  Questa impostazione definisce l’ambito di una scansione on-demand. È possibile specificare le dimensioni massime dei file da sottoporre a scansione, le estensioni e i percorsi dei file da includere nella scansione e le estensioni e i percorsi dei file da escludere dalla scansione. Per impostazione predefinita, i file nelle sottodirectory vengono sottoposti a scansione.

  Si utilizza una pianificazione cron per specificare quando eseguire l’attività. È possibile utilizzare `vserver vscan on-demand-task run` per eseguire l’attività immediatamente.

- **Profilo delle operazioni del file Vscan (solo scansione all’accesso)**

  Il `vscan-fileop-profile` parametro per `vserver cifs share create` Il comando definisce quali operazioni di file SMB attivano la scansione dei virus. Per impostazione predefinita, il parametro è impostato su `standard`, Che è la Best practice di NetApp. È possibile regolare questo parametro in base alle necessità quando si crea o si modifica una condivisione SMB:

  - `no-scan` specifica che le scansioni antivirus non vengono mai attivate per la condivisione.
  - `standard` specifica che le scansioni antivirus vengono attivate da operazioni di apertura, chiusura e ridenominazione.
  - `strict` specifica che le scansioni antivirus vengono attivate da operazioni di apertura, lettura, chiusura e ridenominazione.

    Il `strict` profile offre una maggiore sicurezza per le situazioni in cui più client accedono a un file contemporaneamente. Se un client chiude un file dopo averlo scritto e lo stesso file rimane aperto su un secondo client, `strict` garantisce che un’operazione di lettura sul secondo client attivi una scansione prima della chiusura del file.

    Fare attenzione a limitare il `strict` il profilo alle condivisioni contenenti file che prevedi sia accessibile contemporaneamente. Poiché questo profilo genera più richieste di scansione, potrebbe avere un impatto sulle performance.

  - `writes-only` specifica che le scansioni antivirus vengono attivate solo quando i file modificati vengono chiusi.

    Da `writes-only` genera meno richieste di scansione, in genere migliora le performance.

Se si utilizza questo profilo, lo scanner deve essere configurato per eliminare o mettere in quarantena i file infetti non riparabili, in modo che non sia possibile accedervi. Se, ad esempio, un client chiude un file dopo la scrittura di un virus e il file non viene riparato, eliminato o messo in quarantena, qualsiasi client che accede al file `without` la scrittura su di esso sarà infetto.

> Se un'applicazione client esegue un'operazione di ridenominazione, il file viene chiuso con il nuovo nome e non viene sottoposto a scansione. Se tali operazioni rappresentano un problema di sicurezza nell'ambiente in uso, è necessario utilizzare `standard` oppure `strict` profilo.

Soluzioni partner di Vscan

NetApp collabora con Trellix, Symantec, Trend Micro e Sentinel One per offrire soluzioni anti-malware e anti-virus leader del settore basate sulla tecnologia ONTAP Vscan. Queste soluzioni consentono di eseguire la scansione dei file per rilevare la presenza di malware e correggere eventuali file interessati.

Come mostrato nella tabella seguente, i dettagli relativi all'interoperabilità per Trellix, Symantec e Trend Micro sono conservati nella matrice di interoperabilità NetApp. I dettagli sull'interoperabilità per Trellix e Symantec sono disponibili anche sui siti Web dei partner. I dettagli sull'interoperabilità di Sentinel One e degli altri nuovi partner verranno gestiti dal partner sui propri siti Web.

Partner	Documentazione della soluzione	Dettagli sull'interoperabilità
Trellix (precedentemente McAfee)	"Documentazione del prodotto Trellix"	• "Tool di matrice di interoperabilità NetApp" • "Piattaforme supportate per Endpoint Security Storage Protection (trellix.com)"
Symantec	"Symantec Protection Engine 9.0.0"	• "Tool di matrice di interoperabilità NetApp" • "Matrice di supporto per dispositivi partner certificati con Symantec Protection Engine (SPE) per NAS (Network Attached Storage) 9.x.x" • "Matrice di supporto per i dispositivi partner certificata con Symantec Protection Engine (SPE) per NAS (Network Attached Storage) 8.x (broadcom.com)"
Trend Micro	"Guida introduttiva di Trend Micro ServerProtect for Storage 6.0"	"Tool di matrice di interoperabilità NetApp"

Partner	Documentazione della soluzione	Dettagli sull'interoperabilità
Sentinel One	• "SentinelOne Singularity Cloud Data Security" • "Supporto SentinelOne" Questo collegamento richiede l'accesso dell'utente. È possibile richiedere l'accesso da Sentinel One.	Istinto profondo

Installazione e configurazione del server Vscan

Installazione e configurazione del server Vscan

Impostare uno o più server Vscan per verificare che i file sul sistema vengano sottoposti a scansione antivirus. Seguire le istruzioni fornite dal fornitore per installare e configurare il software antivirus sul server.

Seguire le istruzioni contenute nel file README fornito da NetApp per installare e configurare il connettore antivirus ONTAP. In alternativa, seguire le istruzioni sul "Pagina installare il connettore antivirus ONTAP".

> Per le configurazioni di disaster recovery e MetroCluster, è necessario configurare server Vscan separati per i cluster ONTAP primario/locale e secondario/partner.

Requisiti del software antivirus

- Per informazioni sui requisiti del software antivirus, consultare la documentazione del vendor.
- Per informazioni su vendor, software e versioni supportate da Vscan, consultare "Soluzioni partner di Vscan" pagina.

Requisiti del connettore antivirus ONTAP

- È possibile scaricare il connettore antivirus ONTAP dalla pagina **Download software** sul sito di supporto NetApp. "Download NetApp: Software"
- Per informazioni sulle versioni di Windows supportate dal connettore antivirus ONTAP e sui requisiti di interoperabilità, vedere "Soluzioni partner di Vscan".

> È possibile installare diverse versioni dei server Windows per diversi server Vscan in un cluster.

- Sul server Windows deve essere installato .NET 3.0 o versione successiva.
- SMB 2.0 deve essere attivato sul server Windows.

Installare il connettore antivirus ONTAP

Installare il connettore antivirus ONTAP sul server Vscan per abilitare la comunicazione tra il sistema che esegue ONTAP e il server Vscan. Una volta installato il connettore antivirus ONTAP, il software antivirus è in grado di comunicare con una o più Storage

Virtual Machine (SVM).

A proposito di questa attività

- Vedere "Soluzioni partner di Vscan" Per informazioni sui protocolli supportati, le versioni del software dei fornitori antivirus, le versioni di ONTAP, i requisiti di interoperabilità e i server Windows.
- È necessario installare .NET 4.5.1 o versione successiva.
- Il connettore antivirus ONTAP può essere eseguito su una macchina virtuale. Tuttavia, per ottenere prestazioni ottimali, NetApp consiglia di utilizzare una macchina virtuale dedicata per la scansione antivirus.
- SMB 2,0 deve essere attivato sul server Windows su cui si sta installando ed eseguendo il connettore antivirus ONTAP.

Prima di iniziare

- Scaricare il file di installazione di ONTAP Antivirus Connector dal sito di assistenza e salvarlo in una directory sul disco rigido.
- Verificare di soddisfare i requisiti per l'installazione del connettore antivirus ONTAP.
- Verificare di disporre dei privilegi di amministratore per installare il connettore antivirus.

Fasi

1. Avviare l'installazione guidata del connettore antivirus eseguendo il file di installazione appropriato.
2. Selezionare *Avanti*. Viene visualizzata la finestra di dialogo cartella di destinazione.
3. Selezionare *Avanti* per installare il connettore antivirus nella cartella elencata oppure selezionare *Cambia* per eseguire l'installazione in una cartella diversa.
4. Viene visualizzata la finestra di dialogo credenziali servizio Windows connettore AV ONTAP.
5. Immettere le credenziali del servizio Windows o selezionare **Aggiungi** per selezionare un utente. Per un sistema ONTAP, questo utente deve essere un utente di dominio valido e deve esistere nella configurazione del pool di scanner per la SVM.
6. Selezionare **Avanti**. Viene visualizzata la finestra di dialogo Pronto per l'installazione del programma.
7. Selezionare **Installa** per avviare l'installazione o selezionare **Indietro** se si desidera apportare modifiche alle impostazioni.
   Viene visualizzata una finestra di stato che illustra l'avanzamento dell'installazione, seguita dalla finestra di dialogo InstallShield Wizard Completed (Installazione guidata InstallShield completata).
8. Selezionare la casella di controllo Configura LIF ONTAP per continuare con la configurazione di LIF dati o gestione ONTAP.
   Devi configurare almeno una gestione ONTAP o un'interfaccia LIF dati prima che questo server Vscan possa essere utilizzato.
9. Selezionare la casella di controllo Mostra registro **Windows Installer** se si desidera visualizzare i registri di installazione.
10. Selezionare **fine** per terminare l'installazione e chiudere la procedura guidata InstallShield.
    L'icona **Configura LIF ONTAP** viene salvata sul desktop per configurare le LIF ONTAP.
11. Aggiungere una SVM al connettore antivirus.
    Puoi aggiungere una SVM al connettore antivirus aggiungendo una LIF di gestione ONTAP, che viene interrogata per recuperare l'elenco di LIF dati, oppure configurando direttamente la LIF o la LIF dati.
    Se la LIF di gestione ONTAP è configurata, devi anche fornire le informazioni di polling e le credenziali dell'account amministratore di ONTAP.
    - Verifica che la LIF di gestione o l'indirizzo IP della SVM sia abilitato per `management-https`. Non è

necessario quando si configurano solo LIF dati.

- Verificare di aver creato un account utente per l'applicazione HTTP e di aver assegnato un ruolo con accesso (almeno di sola lettura) a `/api/network/ip/interfaces` API REST.
  Per ulteriori informazioni sulla creazione di un utente, vedere la "creazione del ruolo di accesso di sicurezza" e. "creazione dell'accesso di sicurezza" Pagine man di ONTAP.

> Puoi anche utilizzare l'utente di dominio come account aggiungendo una SVM con tunnel di autenticazione per una SVM amministrativa. Per ulteriori informazioni, consultare "login di sicurezza creazione del tunnel di dominio" Pagina man di ONTAP o utilizzare `/api/security/acccounts` e. `/api/security/roles` REST API per configurare l'account e il ruolo di amministratore.

Fasi

1. Fare clic con il pulsante destro del mouse sull'icona **Configure ONTAP LIF**, salvata sul desktop al termine dell'installazione di Antivirus Connector, quindi selezionare **Esegui come amministratore**.
2. Nella finestra di dialogo Configura LIF ONTAP, selezionare il tipo di configurazione preferito, quindi eseguire le seguenti operazioni:

Per creare questo tipo di LIF…	Eseguire questa procedura…
LIF dati	a. Impostare "ruolo" su "dati" b. Impostare "protocollo dati" su "cifs" c. Impostare "policy firewall" su "data" d. Impostare "politica di servizio" su "file-dati-predefiniti"
LIF di gestione	a. Impostare "ruolo* su "dati" b. Impostare "protocollo dati" su "nessuno" c. Impostare "policy firewall" su "Mgmt" d. Impostare "politica di servizio" su "gestione predefinita"

Scopri di più "Creazione di una LIF".

Dopo aver creato una LIF, inserisci i dati o l'indirizzo IP della LIF di gestione o della SVM che desideri aggiungere. Puoi anche inserire la LIF di gestione cluster. Se specifichi la LIF di gestione cluster, tutte le SVM del cluster che servono SMB potranno utilizzare il server Vscan.

> Quando è richiesta l'autenticazione Kerberos per i server Vscan, ogni LIF dati SVM deve avere un nome DNS univoco ed è necessario registrarlo come nome principale server (SPN) con Windows Active Directory. Quando non è disponibile un nome DNS univoco per ogni LIF dati o registrato come SPN, il server Vscan utilizza il meccanismo NT LAN Manager per l'autenticazione. Se si aggiungono o modificano i nomi DNS e gli SPN dopo la connessione del server Vscan, è necessario riavviare il servizio Antivirus Connector sul server Vscan per applicare le modifiche.

3. Per configurare una LIF di gestione, inserisci la durata del polling in secondi. La durata del poll è la frequenza con cui il connettore antivirus verifica le modifiche alle SVM o alla configurazione LIF del cluster. L'intervallo di polling predefinito è di 60 secondi.
4. Inserisci il nome dell'account e la password dell'amministratore ONTAP per configurare una LIF di

gestione.

5. Fare clic su **Test** per controllare la connettività e verificare l'autenticazione. L'autenticazione viene verificata solo per una configurazione LIF di gestione.
6. Fare clic su **Update** (Aggiorna) per aggiungere la LIF all'elenco delle LIF a cui eseguire il polling o connettersi.
7. Fare clic su **Salva** per salvare la connessione al Registro di sistema.
8. Fare clic su **Esporta** se si desidera esportare l'elenco delle connessioni in un file di importazione del Registro di sistema o di esportazione del Registro di sistema. Ciò è utile se più server Vscan utilizzano lo stesso set di LIF di gestione o di dati.

Vedere "Configurare la pagina ONTAP Antivirus Connector" per le opzioni di configurazione.

Configurare il connettore antivirus ONTAP

Configurare il connettore antivirus ONTAP per specificare una o più Storage Virtual Machine (SVM) a cui connettersi inserendo la LIF di gestione ONTAP, le informazioni di polling e le credenziali dell'account amministratore ONTAP o solo la LIF dati. Puoi anche modificare i dettagli di una connessione SVM o rimuovere una connessione SVM. Per impostazione predefinita, il connettore antivirus ONTAP utilizza le API REST per recuperare l'elenco di LIF di dati, se la LIF di gestione ONTAP è configurata.

Modificare i dettagli di una connessione SVM

Puoi aggiornare i dettagli di una connessione SVM (Storage Virtual Machine), che è stata aggiunta al connettore antivirus, modificando la LIF di gestione ONTAP e le informazioni di polling. Non puoi aggiornare le LIF dati dopo che sono state aggiunte. Per aggiornare le LIF dati, devi prima rimuoverle e poi aggiungerle di nuovo con il nuovo indirizzo LIF o IP.

Prima di iniziare

Verificare di aver creato un account utente per l'applicazione HTTP e di aver assegnato un ruolo con accesso (almeno di sola lettura) a `/api/network/ip/interfaces` API REST.
Per ulteriori informazioni sulla creazione di un utente, vedere la "creazione del ruolo di accesso di sicurezza" e a. "creazione dell'accesso di sicurezza" comandi.
Puoi anche utilizzare l'utente di dominio come account aggiungendo una SVM con tunnel di autenticazione per una SVM amministrativa.
Per ulteriori informazioni, consultare "login di sicurezza creazione del tunnel di dominio" Pagina man di ONTAP.

Fasi

1. Fare clic con il pulsante destro del mouse sull'icona **Configura LIF ONTAP**, salvata sul desktop al termine dell'installazione di Antivirus Connector, quindi selezionare **Esegui come amministratore**. Viene visualizzata la finestra di dialogo Configura LIF ONTAP.
2. Selezionare l'indirizzo IP della SVM, quindi fare clic su **Aggiorna**.
3. Aggiornare le informazioni secondo necessità.
4. Fare clic su **Salva** per aggiornare i dettagli della connessione nel registro.
5. Fare clic su **Esporta** se si desidera esportare l'elenco delle connessioni in un'importazione del Registro di sistema o in un file di esportazione del Registro di sistema.
   Ciò è utile se più server Vscan utilizzano lo stesso set di LIF di gestione o di dati.

Rimuovere una connessione SVM dal connettore antivirus

Se non ti serve più una connessione SVM, puoi rimuoverla.

Fasi

1. Fare clic con il pulsante destro del mouse sull'icona **Configura LIF ONTAP**, salvata sul desktop al termine dell'installazione di Antivirus Connector, quindi selezionare **Esegui come amministratore**. Viene visualizzata la finestra di dialogo Configura LIF ONTAP.
2. Selezionare uno o più indirizzi IP SVM, quindi fare clic su **Rimuovi**.
3. Fare clic su **Salva** per aggiornare i dettagli della connessione nel registro.
4. Fare clic su **Esporta** se si desidera esportare l'elenco delle connessioni in un file di importazione del Registro di sistema o di esportazione del Registro di sistema.
   Ciò è utile se più server Vscan utilizzano lo stesso set di LIF di gestione o di dati.

Risolvere i problemi

Prima di iniziare

Quando si creano i valori del Registro di sistema in questa procedura, utilizzare il riquadro a destra.

È possibile attivare o disattivare i registri dei connettori antivirus per scopi diagnostici. Per impostazione predefinita, questi registri sono disattivati. Per migliorare le prestazioni, è necessario disattivare i registri del connettore antivirus e attivarli solo per gli eventi critici.

Fasi

1. Selezionare **Start**, digitare "regedit" nella casella di ricerca, quindi selezionare `regedit.exe` Nell'elenco programmi.
2. In **Editor del Registro di sistema**, individuare la seguente sottochiave per il connettore antivirus ONTAP: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Creare i valori del Registro di sistema specificando il tipo, il nome e i valori indicati nella tabella seguente:

Tipo	Nome	Valori
Stringa	Tracepath	c:\avshim.log

   Questo valore del Registro di sistema potrebbe essere qualsiasi altro percorso valido.

4. Creare un altro valore del Registro di sistema fornendo il tipo, il nome, i valori e le informazioni di registrazione mostrate nella tabella seguente:

Tipo	Nome	Registrazione critica	Registrazione intermedia	Registrazione dettagliata
DWORD	TRACELEVEL	1	2 o 3	4

   In questo modo si attivano i registri del connettore antivirus salvati al valore del percorso fornito in TracePath nel passaggio 3.

5. Disattivare i registri del connettore antivirus eliminando i valori del Registro di sistema creati nei passaggi 3 e 4.

6. Creare un altro valore di registro di tipo "MULTI_SZ" con il nome "LogRotation" (senza virgolette). In "LogRotation",
   Fornire "logFileSize:1" come voce per la dimensione di rotazione (dove 1 rappresenta 1MB) e nella riga successiva fornire "logFileCount:5" come un
   immissione del limite di rotazione (5 è il limite).

> Questi valori sono facoltativi. Se non vengono forniti, vengono utilizzati i valori predefiniti dei file 20MB e 10 rispettivamente per la dimensione di rotazione e il limite di rotazione. I valori interi forniti non forniscono valori decimali o frazioni. Se si forniscono valori superiori ai valori predefiniti, vengono utilizzati i valori predefiniti.

7. Per disattivare la rotazione del registro configurata dall'utente, eliminare i valori del Registro di sistema creati nel passaggio 6.

Banner personalizzabile

Un banner personalizzato ti consente di inserire un'istruzione legale e un'esclusione di responsabilità per l'accesso al sistema nella finestra *Configure ONTAP LIF API*.

Fase

1. Modificare l'intestazione predefinita aggiornando il contenuto della `banner.txt` nella directory di installazione, quindi salvare le modifiche.
   Riapri la finestra Configura API LIF ONTAP per vedere le modifiche riflesse nel banner.

Attivare la modalità Extended Ordinance (EO)

È possibile attivare e disattivare la modalità Extended Ordinance (EO) per garantire un funzionamento sicuro.

Fasi

1. Selezionare **Start**, digitare "regedit" nella casella di ricerca, quindi selezionare `regedit.exe` Nell'elenco programmi.
2. In **Editor del Registro di sistema**, individuare la seguente sottochiave per ONTAP Antivirus Connector: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Nel riquadro a destra, creare un nuovo valore del Registro di sistema di tipo "DWORD" con il nome "EO_Mode" (senza virgolette) e il valore "1" (senza virgolette) per attivare la modalità EO o il valore "0" (senza virgolette) per disattivare la modalità EO.

> Per impostazione predefinita, se `EO_Mode` La voce del Registro di sistema è assente, la modalità EO è disattivata. Quando si attiva la modalità EO, è necessario configurare sia il server syslog esterno che l'autenticazione dei certificati reciproci.

Configurare il server syslog esterno

Prima di iniziare

Tenere presente che quando si creano i valori del Registro di sistema in questa procedura, utilizzare il riquadro a destra.

Fasi

1. Selezionare **Start**, digitare "regedit" nella casella di ricerca, quindi selezionare `regedit.exe` Nell'elenco programmi.

2. In **Editor del Registro di sistema**, creare la seguente sottochiave per ONTAP Antivirus Connector per la configurazione syslog:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Creare un valore del Registro di sistema specificando il tipo, il nome e il valore come illustrato nella tabella seguente:

Tipo	Nome	Valore
DWORD	syslog_enabled	1 o 0

   Si noti che un valore "1" attiva il syslog e un valore "0" lo disattiva.

4. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome
REG_SZ	Syslog_host

   Fornire l'indirizzo IP dell'host syslog o il nome di dominio per il campo valore.

5. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome
REG_SZ	Porta_syslog

   Specificare il numero della porta su cui viene eseguito il server syslog nel campo Value.

6. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome
REG_SZ	Syslog_Protocol

   Immettere il protocollo in uso sul server syslog, "tcp" o "udp", nel campo valore.

7. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome	LOG_CRIT	LOG_NOTICE	LOG_INFO	LOG_DEBUG
DWORD	Syslog_level	2	5	6	7

8. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome	Valore
DWORD	syslog_tls	1 o 0

Si noti che un valore "1" abilita syslog con TLS (Transport Layer Security) e un valore "0" disabilita syslog con TLS.

Garantire il corretto funzionamento di un server syslog esterno configurato

- Se la chiave è assente o ha un valore nullo:
  - L'impostazione predefinita del protocollo è "tcp".
  - L'impostazione predefinita della porta è "514" per "tcp/udp" e "6514" per TLS.
  - Il livello syslog predefinito è 5 (LOG_NOTICE).
- Puoi confermare che syslog è attivato verificando che `syslog_enabled` il valore è "1". Quando il `syslog_enabled` Il valore è "1", dovrebbe essere possibile accedere al server remoto configurato indipendentemente dall'attivazione o meno della modalità EO.
- Se la modalità EO è impostata su "1" e si modifica la `syslog_enabled` valore compreso tra "1" e "0", vale quanto segue:
  - Non è possibile avviare il servizio se syslog non è abilitato in modalità EO.
  - Se il sistema è in esecuzione in modalità regolare, viene visualizzato un avviso che indica che syslog non può essere disattivato in modalità EO e che syslog è impostato con forza su "1", che è possibile vedere nel Registro di sistema. In questo caso, è necessario disattivare prima la modalità EO e poi disabilitare syslog.
- Se il server syslog non è in grado di funzionare correttamente quando la modalità EO e syslog sono attivati, il servizio si arresta. Questo può verificarsi per uno dei seguenti motivi:
  - È stato configurato un syslog_host non valido o non esistente.
  - È stato configurato un protocollo non valido tranne UDP o TCP.
  - Un numero di porta non è valido.
- Per una configurazione TCP o TLS su TCP, se il server non è in ascolto sulla porta IP, la connessione non riesce e il servizio si arresta.

Configurare l'autenticazione reciproca dei certificati X,509

L'autenticazione reciproca basata su certificati X,509 è possibile per la comunicazione SSL (Secure Sockets Layer) tra il connettore antivirus e ONTAP nel percorso di gestione. Se la modalità EO è attivata e il certificato non viene trovato, il connettore AV termina. Eseguire la seguente procedura sul connettore dell'antivirus:

Fasi

1. Il connettore antivirus ricerca il certificato client del connettore antivirus e il certificato dell'autorità di certificazione (CA) per il server NetApp nel percorso di directory da cui il connettore antivirus esegue la directory di installazione. Copiare i certificati in questo percorso di directory fisso.
2. Incorporare il certificato client e la relativa chiave privata nel formato PKCS12 e denominarlo "AV_client.P12".
3. Verificare che il certificato CA (insieme a qualsiasi autorità di firma intermedia fino alla CA principale) utilizzato per firmare il certificato per il server NetApp sia in formato PEM (Privacy Enhanced Mail) e denominato "ONTAP_CA.pem". Posizionarlo nella directory di installazione di Antivirus Connector. Sul sistema NetApp ONTAP, installare il certificato CA (insieme a qualsiasi autorità di firma intermedia fino alla CA principale) utilizzato per firmare il certificato client per il connettore antivirus in "ONTAP" come certificato di tipo "client-ca".

Configurare i pool di scanner

Panoramica sulla configurazione dei pool di scanner

Un pool di scanner definisce i server Vscan e gli utenti con privilegi che possono connettersi alle SVM. Un criterio dello scanner determina se un pool di scanner è attivo.

> Se si utilizza un criterio di esportazione su un server SMB, è necessario aggiungere ciascun server Vscan al criterio di esportazione.

Creare un pool di scanner su un singolo cluster

Un pool di scanner definisce i server Vscan e gli utenti con privilegi che possono connettersi alle SVM. È possibile creare un pool di scanner per una singola SVM o per tutte le SVM in un cluster.

Di cosa hai bisogno

- I server SVM e Vscan devono trovarsi nello stesso dominio o in domini attendibili.
- Per i pool di scanner definiti per una singola SVM, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione SVM o la LIF dei dati SVM.
- Per i pool di scanner definiti per tutte le SVM in un cluster, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione del cluster.
- L'elenco degli utenti con privilegi deve includere l'account utente di dominio utilizzato dal server Vscan per connettersi a SVM.
- Una volta configurato il pool di scanner, controllare lo stato della connessione ai server.

Fasi

1. Creazione di un pool di scanner:

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - Specificare una SVM di dati per un pool definito per una singola SVM e specificare una SVM amministrativa del cluster per un pool definito per tutte le SVM in un cluster.
   - Specificare un indirizzo IP o un FQDN per ciascun nome host del server Vscan.
   - Specificare il dominio e il nome utente per ciascun utente con privilegi. Per un elenco completo delle opzioni, vedere la pagina man del comando.

     Il seguente comando crea un pool di scanner denominato `SP` su `vs1` SVM:

   ```
   cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
   SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
   cifs\u1,cifs\u2
   ```

2. Verificare che il pool di scanner sia stato creato:

`vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli di `SP` pool di scanner:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: idle
                            Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

È inoltre possibile utilizzare `vserver vscan scanner-pool show` Per visualizzare tutti i pool di scanner su una SVM. Per la sintassi completa dei comandi, vedere la pagina man del comando.

Creazione di pool di scanner nelle configurazioni MetroCluster

È necessario creare pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster, corrispondente alle SVM primarie e secondarie sul cluster.

Di cosa hai bisogno

- I server SVM e Vscan devono trovarsi nello stesso dominio o in domini attendibili.
- Per i pool di scanner definiti per una singola SVM, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione SVM o la LIF dei dati SVM.
- Per i pool di scanner definiti per tutte le SVM in un cluster, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione del cluster.
- L'elenco degli utenti con privilegi deve includere l'account utente di dominio utilizzato dal server Vscan per connettersi a SVM.
- Una volta configurato il pool di scanner, controllare lo stato della connessione ai server.

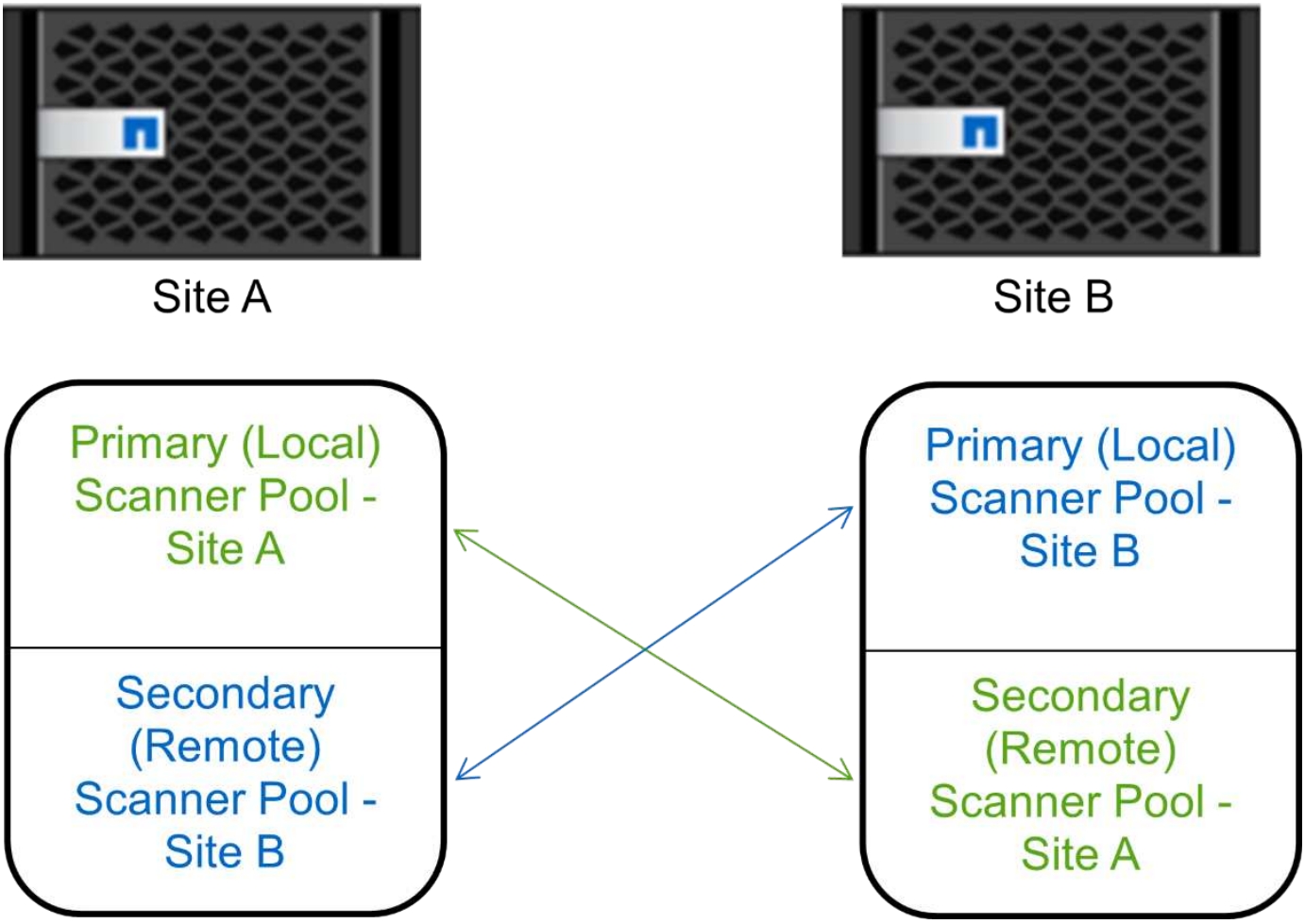
A proposito di questa attività

Le configurazioni MetroCluster proteggono i dati implementando due cluster mirrorati fisicamente separati. Ciascun cluster replica in modo sincrono i dati e la configurazione SVM dell'altro. Una SVM primaria sul cluster locale serve i dati quando il cluster è online. Una SVM secondaria sul cluster locale serve i dati quando il cluster remoto non è in linea.

Ciò significa che è necessario creare pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster, il pool secondario diventa attivo quando il cluster inizia a servire i dati dalla SVM

secondaria. Per il disaster recovery (DR), la configurazione è simile a quella di MetroCluster.

Questa figura mostra una tipica configurazione MetroCluster/DR.



Fasi

1. Creazione di un pool di scanner:

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - Specificare una SVM di dati per un pool definito per una singola SVM e specificare una SVM amministrativa del cluster per un pool definito per tutte le SVM in un cluster.
   - Specificare un indirizzo IP o un FQDN per ciascun nome host del server Vscan.
   - Specificare il dominio e il nome utente per ciascun utente con privilegi.

     È necessario creare tutti i pool di scanner dal cluster contenente la SVM primaria.

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   I seguenti comandi creano pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster:

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. Verificare che i pool di scanner siano stati creati:

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli del pool di scanner `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                   Vserver: cifssvm1
                              Scanner Pool: pool1_for_site1
                            Applied Policy: idle
                            Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

   È inoltre possibile utilizzare `vserver vscan scanner-pool show` Per visualizzare tutti i pool di scanner su una SVM. Per la sintassi completa dei comandi, vedere la pagina man del comando.

Applicare un criterio scanner a un singolo cluster

Un criterio dello scanner determina se un pool di scanner è attivo. È necessario attivare un pool di scanner prima che i server Vscan definiti possano connettersi a una SVM.

A proposito di questa attività

- È possibile applicare un solo criterio scanner a un pool di scanner.
- Se è stato creato un pool di scanner per tutte le SVM in un cluster, è necessario applicare un criterio di scanner a ciascuna SVM singolarmente.

Fasi

1. Applicare un criterio scanner:

   `vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool scanner_pool -scanner-policy primary|secondary|idle -cluster cluster_to_apply_policy_on`

   Un criterio dello scanner può avere uno dei seguenti valori:

   - `Primary` specifica che il pool di scanner è attivo.
   - `Secondary` Specifica che il pool di scanner è attivo solo se nessuno dei server Vscan nel pool di scanner primario è connesso.
   - `Idle` specifica che il pool di scanner non è attivo.

     Nell'esempio seguente viene indicato il nome del pool di scanner `SP` su `vs1` SVM è attivo:

   ```
   cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
   -scanner-pool SP  -scanner-policy primary
   ```

2. Verificare che il pool di scanner sia attivo:

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli di `SP` pool di scanner:

   ```
   cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
   SP

                                       Vserver: vs1
                                  Scanner Pool: SP
                               Applied Policy: primary
                               Current Status: on
            Cluster on Which Policy Is Applied: cluster1
                     Scanner Pool Config Owner: vserver
          List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
   List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
   27.fsct.nb
                      List of Privileged Users: cifs\u1, cifs\u2
   ```

È possibile utilizzare `vserver vscan scanner-pool show-active` Per visualizzare i pool di scanner attivi su una SVM. Per la sintassi completa del comando, vedere la pagina man del comando.

Applicare i criteri dello scanner nelle configurazioni MetroCluster

Un criterio dello scanner determina se un pool di scanner è attivo. È necessario applicare un criterio dello scanner ai pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster.

A proposito di questa attività

- È possibile applicare un solo criterio scanner a un pool di scanner.
- Se è stato creato un pool di scanner per tutte le SVM in un cluster, è necessario applicare un criterio di scanner a ciascuna SVM singolarmente.
- Per le configurazioni di disaster recovery e MetroCluster, è necessario applicare un criterio dello scanner a ogni pool di scanner nel cluster locale e nel cluster remoto.
- Nel criterio creato per il cluster locale, è necessario specificare il cluster locale in `cluster` parametro. Nel criterio creato per il cluster remoto, è necessario specificare il cluster remoto in `cluster` parametro. Il cluster remoto può quindi rilevare le operazioni di scansione dei virus in caso di disastro.

Fasi

1. Applicare un criterio scanner:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   Un criterio dello scanner può avere uno dei seguenti valori:

   - `Primary` specifica che il pool di scanner è attivo.
   - `Secondary` Specifica che il pool di scanner è attivo solo se nessuno dei server Vscan nel pool di scanner primario è connesso.
   - `Idle` specifica che il pool di scanner non è attivo.

     > È necessario applicare tutti i criteri dello scanner dal cluster contenente la SVM primaria.

     I seguenti comandi applicano i criteri dello scanner ai pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster:

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. Verificare che il pool di scanner sia attivo:

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli del pool di scanner `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                   Vserver: cifssvm1
                              Scanner Pool: pool1_for_site1
                            Applied Policy: primary
                            Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

   È possibile utilizzare `vserver vscan scanner-pool show-active` Per visualizzare i pool di scanner attivi su una SVM. Per la sintassi completa dei comandi, vedere la pagina man del comando.

Comandi per la gestione dei pool di scanner

È possibile modificare ed eliminare i pool di scanner e gestire gli utenti con privilegi e i server Vscan per un pool di scanner. È inoltre possibile visualizzare informazioni riepilogative sul pool di scanner.

Se si desidera…	Immettere il seguente comando…
Modificare un pool di scanner	`vserver vscan scanner-pool modify`
Eliminare un pool di scanner	`vserver vscan scanner-pool delete`
Aggiungere utenti con privilegi a un pool di scanner	`vserver vscan scanner-pool privileged-users add`
Eliminare gli utenti con privilegi da un pool di scanner	`vserver vscan scanner-pool privileged-users remove`
Aggiungere server Vscan a un pool di scanner	`vserver vscan scanner-pool servers add`
Eliminare i server Vscan da un pool di scanner	`vserver vscan scanner-pool servers remove`
Visualizza riepilogo e dettagli di un pool di scanner	`vserver vscan scanner-pool show`
Visualizzare gli utenti con privilegi per un pool di scanner	`vserver vscan scanner-pool privileged-users show`
Visualizzare i server Vscan per tutti i pool di scanner	`vserver vscan scanner-pool servers show`

Per ulteriori informazioni su questi comandi, consulta le pagine man.

Configurare la scansione on-access

Creare una policy di accesso

Un criterio di accesso definisce l'ambito di una scansione all'accesso. È possibile creare una policy di accesso per una singola SVM o per tutte le SVM in un cluster. Se è stata creata una policy di accesso per tutte le SVM in un cluster, è necessario attivare la policy su ogni SVM singolarmente.

A proposito di questa attività

- È possibile specificare le dimensioni massime dei file da sottoporre a scansione, le estensioni e i percorsi dei file da includere nella scansione e le estensioni e i percorsi dei file da escludere dalla scansione.
- È possibile impostare `scan-mandatory` Selezionare Off per specificare che l'accesso al file è consentito quando non sono disponibili server Vscan per la scansione dei virus.
- Per impostazione predefinita, ONTAP crea una policy di accesso denominata "default_CIFS" e la abilita per tutte le SVM in un cluster.
- Qualsiasi file idoneo per l'esclusione della scansione in base a. `paths-to-exclude`, `file-ext-to-exclude`, o. `max-file-size` i parametri non vengono presi in considerazione per la scansione, anche se `scan-mandatory` l'opzione è impostata su on. (Selezionare questa opzione "risoluzione dei problemi" sezione per i problemi di connettività relativi a. `scan-mandatory` opzione).

- Per impostazione predefinita, viene eseguita la scansione solo dei volumi di lettura/scrittura. È possibile specificare i filtri che consentono la scansione di volumi di sola lettura o che limitano la scansione ai file aperti con accesso di esecuzione.
- La scansione virus non viene eseguita su una condivisione SMB per la quale il parametro Continuously-Available è impostato su Yes.
- Vedere "Architettura antivirus" Per ulteriori informazioni sul profilo *Vscan file-Operations*.
- È possibile creare un massimo di dieci (10) criteri di accesso per SVM. Tuttavia, è possibile attivare un solo criterio di accesso alla volta.
  - È possibile escludere un massimo di cento (100) percorsi ed estensioni di file dalla scansione virus in una policy di accesso.
- Alcuni consigli sull'esclusione dei file:
  - Considerare l'esclusione di file di grandi dimensioni (è possibile specificare le dimensioni del file) dalla scansione dei virus perché possono causare un rallentamento della risposta o timeout delle richieste di scansione per gli utenti CIFS. La dimensione predefinita del file per l'esclusione è 2 GB.
  - Considerare l'esclusione di estensioni di file come `.vhd` e. `.tmp` perché i file con queste estensioni potrebbero non essere appropriati per la scansione.
  - Considerare l'esclusione di percorsi di file come la directory di quarantena o i percorsi in cui sono memorizzati solo i dischi rigidi o i database virtuali.
  - Verificare che tutte le esclusioni siano specificate nello stesso criterio, in quanto è possibile attivare un solo criterio alla volta. NetApp consiglia di utilizzare lo stesso set di esclusioni specificato nel motore antivirus.
- Per un è necessario un criterio di accesso scansione su richiesta. Per evitare la scansione all'accesso per, è necessario impostare `-scan-files-with-no-ext` a false e. `-file-ext-to-exclude` a * per escludere tutte le estensioni.

Fasi

1. Creare una policy di accesso:

   `vserver vscan on-access-policy create -vserver` *`data_SVM|cluster_admin_SVM`* `-policy-name` *`policy_name`* `-protocol CIFS -max-file-size` *`max_size_of_files_to_scan`* `-filters [scan-ro-volume,][scan-execute-access] -file-ext-to-include` *`extensions_of_files_to_include`* `-file-ext-to-exclude` *`extensions_of_files_to_exclude`* `-scan-files-with-no-ext true|false -paths-to -exclude` *`paths_of_files_to_exclude`* `-scan-mandatory on|off`

   - Specificare una SVM di dati per una policy definita per una singola SVM, una SVM amministrativa del cluster per una policy definita per tutte le SVM in un cluster.
   - Il `-file-ext-to-exclude` l'impostazione ha la precedenza su `-file-ext-to-include` impostazione.
   - Impostare `-scan-files-with-no-ext` a true per eseguire la scansione dei file senza estensioni. Il comando seguente crea una policy di accesso denominata `Policy1` su `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
-name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
-file-ext-to-include “mp*”,"tx*" -file-ext-to-exclude "mp3","txt" -scan
-files-with-no-ext false -paths-to-exclude "\vol\a b\","\vol\a,b\"
```

2. Verificare che il criterio di accesso sia stato creato: `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name name`

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli di `Policy1` policy:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                           Vserver: vs1
                            Policy: Policy1
                     Policy Status: off
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

Attivare un criterio di accesso

Un criterio di accesso definisce l'ambito di una scansione all'accesso. È necessario attivare un criterio di accesso su una SVM prima di poter eseguire la scansione dei relativi file.

Se è stata creata una policy di accesso per tutte le SVM in un cluster, è necessario attivare la policy su ogni SVM singolarmente. È possibile attivare un solo criterio di accesso su una SVM alla volta.

Fasi

1. Attivare una policy di accesso:

   `vserver vscan on-access-policy enable -vserver data_SVM -policy-name policy_name`

   Il comando seguente attiva un criterio di accesso denominato `Policy1` su `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
-name Policy1
```

2. Verificare che il criterio di accesso sia attivato:

   `vserver vscan on-access-policy show -instance data_SVM -policy-name`

policy_name

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli di `Policy1` policy di accesso:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                           Vserver: vs1
                            Policy: Policy1
                     Policy Status: on
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

Modificare il profilo delle operazioni del file Vscan per una condivisione SMB

Il *profilo delle operazioni del file Vscan* per una condivisione SMB definisce le operazioni sulla condivisione che possono attivare la scansione. Per impostazione predefinita, il parametro è impostato su `standard`. È possibile regolare il parametro in base alle necessità quando si crea o si modifica una condivisione SMB.

Vedere "Architettura antivirus" Per ulteriori informazioni sul profilo *Vscan file-Operations*.

> La scansione antivirus non viene eseguita su una condivisione SMB che dispone di `continuously-available` parametro impostato su `Yes`.

Fase

1. Modificare il valore del profilo delle operazioni del file Vscan per una condivisione SMB:

   `vserver cifs share modify -vserver` *`data_SVM`* `-share-name` *`share`* `-path` *`share_path`* `-vscan-fileop-profile no-scan|standard|strict|writes-only`

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando modifica il profilo delle operazioni del file Vscan per una condivisione SMB in `strict`:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name
SALES_SHARE -path /sales -vscan-fileop-profile strict
```

Comandi per la gestione delle policy di accesso

È possibile modificare, disattivare o eliminare un criterio di accesso. È possibile visualizzare un riepilogo e i dettagli della policy.

Se si desidera…	Immettere il seguente comando…
Creare una policy di accesso	`vserver vscan on-access-policy create`
Modificare un criterio di accesso	`vserver vscan on-access-policy modify`
Attivare un criterio di accesso	`vserver vscan on-access-policy enable`
Disattiva un criterio di accesso	`vserver vscan on-access-policy disable`
Eliminare un criterio di accesso	`vserver vscan on-access-policy delete`
Visualizza riepilogo e dettagli per una policy di accesso	`vserver vscan on-access-policy show`
Aggiungere all'elenco di percorsi da escludere	`vserver vscan on-access-policy paths-to-exclude add`
Eliminare dall'elenco dei percorsi da escludere	`vserver vscan on-access-policy paths-to-exclude remove`
Visualizzare l'elenco dei percorsi da escludere	`vserver vscan on-access-policy paths-to-exclude show`
Aggiungere all'elenco delle estensioni di file da escludere	`vserver vscan on-access-policy file-ext-to-exclude add`
Eliminare dall'elenco delle estensioni di file da escludere	`vserver vscan on-access-policy file-ext-to-exclude remove`
Visualizzare l'elenco delle estensioni di file da escludere	`vserver vscan on-access-policy file-ext-to-exclude show`
Aggiungere all'elenco delle estensioni di file da includere	`vserver vscan on-access-policy file-ext-to-include add`

Eliminare dall'elenco delle estensioni di file da includere	`vserver vscan on-access-policy file-ext-to-include remove`
Visualizzare l'elenco delle estensioni di file da includere	`vserver vscan on-access-policy file-ext-to-include show`

Per ulteriori informazioni su questi comandi, consulta le pagine man.

Configurare la scansione on-demand

Configurare una panoramica della scansione on-demand

È possibile utilizzare la scansione on-demand per controllare i file alla ricerca di virus immediatamente o in base a una pianificazione.

Ad esempio, è possibile eseguire scansioni solo in ore non di punta oppure eseguire la scansione di file di grandi dimensioni esclusi da una scansione all'accesso. È possibile utilizzare una pianificazione cron per specificare quando eseguire l'attività.

A proposito di questo argomento

- È possibile assegnare una pianificazione quando si crea un'attività.
- È possibile pianificare una sola attività alla volta su una SVM.
- La scansione on-demand non supporta la scansione di collegamenti simbolici o file di flusso.

> La scansione on-demand non supporta la scansione di collegamenti simbolici o file di flusso.

> Per creare un'attività on-demand, è necessario abilitare almeno una policy di accesso. Può essere il criterio predefinito o un criterio di accesso creato dall'utente.

Crea un'attività on-demand

Un'attività su richiesta definisce l'ambito della scansione antivirus su richiesta. È possibile specificare le dimensioni massime dei file da sottoporre a scansione, le estensioni e i percorsi dei file da includere nella scansione e le estensioni e i percorsi dei file da escludere dalla scansione. Per impostazione predefinita, i file nelle sottodirectory vengono sottoposti a scansione.

A proposito di questa attività

- È possibile eseguire un massimo di dieci (10) task on-demand per ogni SVM, ma è possibile attivarne solo una.
- Un'attività on-demand crea un report contenente informazioni relative alle statistiche relative alle scansioni. Questo report è accessibile con un comando o scaricando il file di report creato dall'attività nella posizione definita.

Prima di iniziare

- Devi avere creazione di un criterio di accesso. Il criterio può essere predefinito o creato dall'utente. Senza il criterio di accesso, non è possibile attivare la scansione.

Fasi

1. Crea un'attività on-demand:

   ```
   vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
   -scan-paths paths_of_files_to_scan -report-directory report_directory_path
   -report-expiry-time expiration_time_for_report -schedule cron_schedule -max
   -file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to
   -exclude file_extensions -file-ext-to-include file_extensions -scan-files-with
   -no-ext true|false -directory-recursion true|false
   ```

   - Il `-file-ext-to-exclude` l'impostazione ha la precedenza su `-file-ext-to-include` impostazione.
   - Impostare `-scan-files-with-no-ext` a true per eseguire la scansione dei file senza estensioni.

     Per un elenco completo delle opzioni, consultare la "riferimento al comando".

     Il seguente comando crea un'attività on-demand denominata `Task1` Sulla `VS1`SVM:

   ```
   cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
   Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
   -schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
   -file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
   -scan-files-with-no-ext false
   [Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
   command to view the status.
   ```

   +

   > È possibile utilizzare `job show` per visualizzare lo stato del lavoro. È possibile utilizzare `job pause` e. `job resume` comandi per mettere in pausa e riavviare il lavoro o l' `job stop` per terminare il lavoro.

2. Verificare che l'attività on-demand sia stata creata:

   ```
   vserver vscan on-demand-task show -instance data_SVM -task-name task_name
   ```

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli di `Task1` attività:

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                           Vserver: vs1
                         Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                      Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                  Report Log Level: info
        Expiration Time for Report: -
```

Al termine

Prima di pianificare l'esecuzione dell'operazione, è necessario attivare la scansione sulla SVM.

Pianificare un'attività on-demand

È possibile creare un'attività senza assegnare una pianificazione e utilizzare `vserver vscan on-demand-task schedule` comando per assegnare un programma o aggiungere un programma durante la creazione dell'attività.

A proposito di questa attività

La pianificazione assegnata con `vserver vscan on-demand-task schedule` il comando sovrascrive un programma già assegnato con `vserver vscan on-demand-task create` comando.

Fasi

1. Pianificare un'attività on-demand:

   `vserver vscan on-demand-task schedule -vserver` *`data_SVM`* `-task-name` *`task_name`* `-schedule cron_schedule`

   Il seguente comando pianifica un'attività di accesso denominata `Task2` su `vs2` SVM:

   ```
   cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
   -name Task2 -schedule daily
   [Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
   command to view the status.
   ```

Per visualizzare lo stato del lavoro, utilizzare `job show` comando. Il `job pause` e. `job resume` i comandi, rispettivamente mettere in pausa e riavviare il lavoro; la `job stop` il comando termina il lavoro.

2. Verificare che l'attività on-demand sia stata pianificata:

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza i dettagli di `Task 2` attività:

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                           Vserver: vs2
                         Task Name: Task2
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                      Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                  Report Log Level: info
```

Al termine

Prima di pianificare l'esecuzione dell'operazione, è necessario attivare la scansione sulla SVM.

Eseguire immediatamente un'attività on-demand

È possibile eseguire un'attività on-demand immediatamente, indipendentemente dal fatto che sia stata assegnata o meno una pianificazione.

Prima di iniziare

È necessario aver attivato la scansione su SVM.

Fase

1. Eseguire immediatamente un'attività on-demand:

   `vserver vscan on-demand-task run -vserver` *`data_SVM`* `-task-name` *`task_name`*

   Il seguente comando esegue un'attività di accesso denominata `Task1` su `vs1` SVM:

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
command to view the status.
```

È possibile utilizzare `job show` per visualizzare lo stato del lavoro. È possibile utilizzare `job pause` e. `job resume` comandi per mettere in pausa e riavviare il lavoro o l' `job stop` per terminare il lavoro.

Comandi per la gestione delle attività on-demand

È possibile modificare, eliminare o annullare la pianificazione di un'attività on-demand. È possibile visualizzare un riepilogo e i dettagli dell'attività e gestire i report per l'attività.

Se si desidera…	Immettere il seguente comando…
Crea un'attività on-demand	`vserver vscan on-demand-task create`
Modificare un'attività on-demand	`vserver vscan on-demand-task modify`
Eliminare un'attività on-demand	`vserver vscan on-demand-task delete`
Eseguire un'attività on-demand	`vserver vscan on-demand-task run`
Pianificare un'attività on-demand	`vserver vscan on-demand-task schedule`
Annulla pianificazione di un'attività on-demand	`vserver vscan on-demand-task unschedule`
Visualizza riepilogo e dettagli per un'attività on-demand	`vserver vscan on-demand-task show`
Visualizza report on-demand	`vserver vscan on-demand-task report show`
Elimina i report on-demand	`vserver vscan on-demand-task report delete`

Per ulteriori informazioni su questi comandi, consulta le pagine man.

Procedure consigliate per la configurazione della funzionalità antivirus off-box in ONTAP

Prendere in considerazione i seguenti consigli per configurare la funzionalità off-box in ONTAP.

- Limitare gli utenti con privilegi alle operazioni di scansione antivirus. Gli utenti normali devono essere scoraggiati dall'utilizzo di credenziali utente con privilegi. Questa restrizione può essere ottenuta disattivando i diritti di accesso per gli utenti con privilegi in Active Directory.
- Gli utenti con privilegi non devono far parte di alcun gruppo di utenti con un elevato numero di diritti nel dominio, ad esempio il gruppo Administrators o il gruppo di operatori di backup. Gli utenti con privilegi devono essere convalidati solo dal sistema di archiviazione in modo che possano creare connessioni al server Vscan e accedere ai file per la scansione antivirus.
- Utilizzare i computer su cui sono in esecuzione i server Vscan solo a scopo di scansione antivirus. Per scoraggiare l'uso generale, disattivare i servizi terminal di Windows e altre disposizioni di accesso remoto su questi computer e concedere il diritto di installare nuovo software su questi computer solo agli amministratori.
- Dedicare i server Vscan alla scansione antivirus e non utilizzarli per altre operazioni, ad esempio i backup. Si potrebbe decidere di eseguire il server Vscan come macchina virtuale (VM). Se si esegue il server Vscan come macchina virtuale, assicurarsi che le risorse assegnate alla macchina virtuale non siano condivise e siano sufficienti per eseguire la scansione antivirus.
- Fornire CPU, memoria e capacità del disco adeguate al server Vscan per evitare un'allocazione eccessiva delle risorse. La maggior parte dei server Vscan è progettata per utilizzare più server core CPU e per distribuire il carico tra le CPU.
- NetApp consiglia di utilizzare una rete dedicata con una VLAN privata per la connessione dalla SVM al server Vscan, in modo che il traffico di scansione non sia influenzato da altro traffico di rete client. Creare una scheda di interfaccia di rete (NIC) separata dedicata alla VLAN antivirus sul server Vscan e alla LIF dati sulla SVM. Questo passaggio semplifica l'amministrazione e la risoluzione dei problemi in caso di problemi di rete. Il traffico antivirus deve essere segregato utilizzando una rete privata. Il server antivirus deve essere configurato per comunicare con il controller di dominio (DC) e ONTAP in uno dei seguenti modi:
  - Il controller di dominio deve comunicare con i server antivirus tramite la rete privata utilizzata per separare il traffico.
  - Il DC e il server antivirus devono comunicare attraverso una rete diversa (non la rete privata menzionata in precedenza), che non è la stessa della rete client CIFS.
  - Per attivare l'autenticazione Kerberos per la comunicazione antivirus, creare una voce DNS per la LIF privata e un nome dell'entità di servizio sul controller di dominio corrispondente alla voce DNS creata per la LIF privata. Usare questo nome quando si aggiunge una LIF al connettore antivirus. Il DNS dovrebbe essere in grado di restituire un nome univoco per ogni LIF privato collegato al connettore antivirus.

> Se la LIF per il traffico Vscan è configurata su una porta diversa dalla LIF per il traffico client, in caso di guasto a una porta la LIF Vscan potrebbe essere sottoposta a failover su un altro nodo. La modifica rende il server Vscan non raggiungibile dal nuovo nodo e le notifiche di scansione per le operazioni sui file sul nodo non riescono. Verificare che il server Vscan sia raggiungibile tramite almeno una LIF su un nodo in modo da poter elaborare le richieste di scansione per le operazioni su file eseguite su quel nodo.

- Collegare il sistema storage NetApp e il server Vscan utilizzando almeno una rete 1GbE.
- Per un ambiente con più server Vscan, collegare tutti i server con connessioni di rete simili ad alte prestazioni. La connessione dei server Vscan migliora le performance consentendo la condivisione del carico.
- Per i siti remoti e le filiali, NetApp consiglia di utilizzare un server Vscan locale piuttosto che un server Vscan remoto, poiché il primo è il candidato ideale per ottenere una latenza elevata. Se il costo è un fattore, utilizzare un notebook o un PC per una protezione antivirus moderata. È possibile pianificare

scansioni periodiche e complete del file system condividendo i volumi o i qtree ed eseguendone la scansione da qualsiasi sistema del sito remoto.

- Utilizzare più server Vscan per eseguire la scansione dei dati sulla SVM a scopo di bilanciamento del carico e ridondanza. La quantità di carico di lavoro CIFS e il conseguente traffico antivirus varia in base alla SVM. Monitorare la latenza di scansione virus e CIFS sullo storage controller. Monitorare l'andamento dei risultati nel tempo. Se la latenza CIFS e la latenza della scansione virus aumentano a causa delle code della CPU o delle applicazioni sui server Vscan oltre le soglie di trend, i client CIFS potrebbero riscontrare lunghi tempi di attesa. Aggiungere altri server Vscan
per distribuire il carico.
- Installare la versione più recente del connettore antivirus ONTAP.
- Mantenere aggiornati i motori e le definizioni antivirus. Consulta i partner per consigli sulla frequenza di aggiornamento.
- In un ambiente multi-tenancy, è possibile condividere un pool di scanner (pool di server Vscan) con più SVM, a condizione che i server Vscan e le SVM facciano parte dello stesso dominio o dominio attendibile.
- Il criterio del software antivirus per i file infetti deve essere impostato su "elimina" o "quarantena", che è il valore predefinito impostato dalla maggior parte dei fornitori di antivirus. Se "vscan-fileop-profile" è impostato su "write_only" e se viene trovato un file infetto, il file rimane nella condivisione e può essere aperto perché l'apertura di un file non attiva una scansione. La scansione antivirus viene attivata solo dopo la chiusura del file.
- Il `scan-engine timeout` il valore deve essere inferiore a. `scanner-pool request-timeout` valore. Se è impostato su un valore più alto, l'accesso ai file potrebbe subire un ritardo e alla fine potrebbe scadere.
  Per evitare questo problema, configurare `scan-engine timeout` a 5 secondi in meno di `scanner-pool request-timeout` valore. Fare riferimento alla documentazione del fornitore del motore di scansione per le istruzioni su come cambiare `scan-engine timeout` impostazioni. Il `scanner-pool timeout` può essere modificato utilizzando il seguente comando in modalità avanzata e fornendo il valore appropriato per `request-timeout` parametro:
  `vserver vscan scanner-pool modify`.
- Per un ambiente dimensionato per i carichi di lavoro di scansione ad accesso e che richiede l'utilizzo di una scansione su richiesta, NetApp consiglia di pianificare il lavoro di scansione su richiesta in orari non di punta per evitare carichi aggiuntivi sull'infrastruttura antivirus esistente.

Scopri di più sulle Best practice specifiche per i partner all'indirizzo "Soluzioni partner di Vscan".

Abilitare la scansione virus su una SVM

È necessario attivare la scansione virus su una SVM prima di eseguire una scansione on-access o on-demand.

Fasi

1. Abilitare la scansione virus su una SVM:

   ```
   vserver vscan enable -vserver data_SVM
   ```

   > È possibile utilizzare `vserver vscan disable` comando per disattivare la scansione virus, se necessario.

   Il seguente comando attiva la scansione virus su `vs1` SVM:

```
cluster1::> vserver vscan enable -vserver vs1
```

2. Verificare che la scansione virus sia attivata su SVM:

   `vserver vscan show -vserver data_SVM`

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando visualizza lo stato Vscan di `vs1` SVM:

```
cluster1::> vserver vscan show -vserver vs1

                          Vserver: vs1
                      Vscan Status: on
```

Ripristinare lo stato dei file sottoposti a scansione

Talvolta, è possibile ripristinare lo stato di scansione dei file sottoposti a scansione su una SVM utilizzando `vserver vscan reset` per eliminare le informazioni memorizzate nella cache per i file. È possibile utilizzare questo comando per riavviare l'elaborazione della scansione virus, ad esempio in caso di una scansione non configurata correttamente.

A proposito di questa attività

Dopo aver eseguito il `vserver vscan reset` comando, tutti i file idonei verranno sottoposti a scansione al successivo accesso.

> Questo comando può influire negativamente sulle prestazioni, a seconda del numero e delle dimensioni dei file da ripetere.

Di cosa hai bisogno

Per questa attività sono richiesti privilegi avanzati.

Fasi

1. Passare al livello di privilegio avanzato:

   `set -privilege advanced`

2. Ripristinare lo stato dei file sottoposti a scansione:

   `vserver vscan reset -vserver data_SVM`

   Il seguente comando ripristina lo stato dei file sottoposti a scansione su `vs1` SVM:

```
cluster1::> vserver vscan reset -vserver vs1
```

Visualizzare le informazioni del registro eventi di Vscan

È possibile utilizzare `vserver vscan show-events` Comando per visualizzare le informazioni del registro eventi relative ai file infetti, agli aggiornamenti dei server Vscan e simili. È possibile visualizzare le informazioni sugli eventi per il cluster o per dati nodi, SVM o server Vscan.

Prima di iniziare

Per visualizzare il registro eventi Vscan sono necessari privilegi avanzati.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Visualizzare le informazioni del registro eventi di Vscan:

   ```
   vserver vscan show-events
   ```

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il comando seguente visualizza le informazioni del registro eventi per il cluster `cluster1`:

   ```
   cluster1::*> vserver vscan show-events

   Vserver     Node            Server          Event Type        Event Time
   ----------- --------------- --------------- -----------------
   -----------------
   vs1         Cluster-01      192.168.1.1     file-infected     9/5/2014
   11:37:38
   vs1         Cluster-01      192.168.1.1     scanner-updated   9/5/2014
   11:37:08
   vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
   11:34:55
   3 entries were displayed.
   ```

Monitoraggio e risoluzione dei problemi di connettività

Potenziali problemi di connettività che coinvolgono l'opzione di scansione obbligatoria

È possibile utilizzare `vserver vscan connection-status show` Comandi per visualizzare informazioni sulle connessioni del server Vscan che potrebbero essere utili per la risoluzione dei problemi di connettività.

Per impostazione predefinita, il `scan-mandatory` L'opzione per la scansione all'accesso nega l'accesso ai file quando non è disponibile una connessione al server Vscan per la scansione. Sebbene questa opzione offra importanti funzioni di sicurezza, può causare problemi in alcune situazioni.

- Prima di abilitare l'accesso client, è necessario assicurarsi che almeno un server Vscan sia connesso a una SVM su ciascun nodo che dispone di una LIF. Se è necessario connettere i server alle SVM dopo aver attivato l'accesso client, è necessario disattivare `scan-mandatory` Opzione su SVM per garantire che l'accesso al file non venga negato perché non è disponibile una connessione al server Vscan. È possibile riattivare l'opzione dopo aver collegato il server.
- Se una LIF di destinazione ospita tutte le connessioni del server Vscan per una SVM, la connessione tra il server e la SVM andrà persa se la LIF viene migrata. Per garantire che l'accesso al file non venga negato perché non è disponibile una connessione al server Vscan, è necessario disattivare `scan-mandatory` Prima di migrare LIF. È possibile riattivare l'opzione dopo la migrazione del LIF.

A ciascuna SVM devono essere assegnati almeno due server Vscan. Si consiglia di collegare i server Vscan al sistema storage su una rete diversa da quella utilizzata per l'accesso client.

Comandi per visualizzare lo stato di connessione del server Vscan

È possibile utilizzare `vserver vscan connection-status show` Comandi per visualizzare informazioni riepilogative e dettagliate sullo stato di connessione del server Vscan.

Se si desidera…	Immettere il seguente comando…
Visualizza un riepilogo delle connessioni del server Vscan	`vserver vscan connection-status show`
Visualizza i dettagli delle connessioni al server Vscan	`vserver vscan connection-status show-all`
Visualizza i dettagli dei server Vscan connessi	`vserver vscan connection-status show-connected`
Visualizza i dettagli dei server Vscan disponibili non connessi	`vserver vscan connection-status show-not-connected`

Per ulteriori informazioni su questi comandi, consultare la "Pagine man di ONTAP".

Risolvere i problemi relativi alla scansione antivirus

Per i problemi più comuni di scansione dei virus, esistono possibili cause e modi per risolverli. La scansione dei virus è nota anche come Vscan.

Problema	Come risolverlo

I server Vscan non sono in grado di connettersi a. Il sistema storage Clustered ONTAP.	Verificare se la configurazione del pool di scanner specifica l'indirizzo IP del server Vscan. Controllare inoltre se gli utenti con privilegi consentiti nell'elenco dei pool di scanner sono attivi. Per controllare il pool di scanner, eseguire `vserver vscan scanner-pool show` al prompt dei comandi del sistema di storage. Se i server Vscan non riescono ancora a connettersi, potrebbe esserci un problema di rete.
I client osservano una latenza elevata.	È probabilmente giunto il momento di aggiungere altri server Vscan al pool di scanner.
Troppe scansioni attivate.	Modificare il valore di `vscan-fileop-profile` parametro per limitare il numero di operazioni sui file monitorate per la scansione antivirus.
Alcuni file non vengono sottoposti a scansione.	Verificare la policy di accesso. È possibile che il percorso di questi file sia stato aggiunto all'elenco di esclusione del percorso o che la loro dimensione superi il valore configurato per le esclusioni. Per verificare il criterio di accesso, eseguire `vserver vscan on-access-policy show` al prompt dei comandi del sistema di storage.
Accesso al file negato.	Controllare se l'impostazione *scan-Mandatory* è specificata nella configurazione dei criteri. Questa impostazione nega l'accesso ai dati se non sono connessi server Vscan. Modificare l'impostazione come necessario.

Monitorare lo stato e le attività delle performance

È possibile monitorare gli aspetti critici del modulo Vscan, ad esempio lo stato di connessione del server Vscan,
Lo stato dei server Vscan e il numero di file sottoposti a scansione. Queste informazioni sono utili
Si diagnosticano i problemi relativi al server Vscan.

Visualizzare le informazioni di connessione del server Vscan

È possibile visualizzare lo stato di connessione dei server Vscan per gestire le connessioni già in uso e le connessioni disponibili per l'utilizzo. I vari comandi visualizzano informazioni
Informazioni sullo stato di connessione dei server Vscan.

Comando…	Informazioni visualizzate…
`vserver vscan connection-status show`	Riepilogo dello stato della connessione

`vserver vscan connection-status show-all`	Informazioni dettagliate sullo stato della connessione
`vserver vscan connection-status show-not-connected`	Stato delle connessioni disponibili ma non connesse
`vserver vscan connection-status show-connected`	Informazioni sul server Vscan collegato

Per ulteriori informazioni su questi comandi, consultare la "pagine man".

Visualizzare le statistiche del server Vscan

È possibile visualizzare le statistiche specifiche del server Vscan per monitorare le prestazioni e diagnosticare i problemi relativi a.
scansione virus. È necessario raccogliere un campione di dati prima di poter utilizzare `statistics show` comando a.
Visualizzare le statistiche del server Vscan.
Per completare un campione di dati, completare la seguente fase:

Fase

1. Eseguire `statistics start` e il `optional statistics` comando di arresto.

Visualizzare le statistiche per le richieste e le latenze del server Vscan

È possibile utilizzare ONTAP `offbox_vscan` Contatori per SVM per monitorare la velocità di Vscan
Le richieste del server inviate e ricevute al secondo e le latenze del server in tutte le Vscan
server. Per visualizzare queste statistiche, completare la seguente fase:

Fase

1. Eseguire la visualizzazione delle statistiche `object offbox_vscan -instance SVM` con il contatori seguenti:

Contatore…	Informazioni visualizzate…
`scan_request_dispatched_rate`	Numero di richieste di scansione virus inviate da ONTAP ai server Vscan al secondo
`scan_noti_received_rate`	Numero di richieste di scansione virus ricevute da ONTAP dai server Vscan al secondo
`dispatch_latency`	Latenza all'interno di ONTAP per identificare un server Vscan disponibile e inviare la richiesta a tale server Vscan
`scan_latency`	Latenza di andata e ritorno da ONTAP al server Vscan, compreso il tempo di esecuzione della scansione

Esempio di statistiche generate da un contatore vscan ONTAP offbox

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
--------------------------------------------------------------------
```

Visualizzare le statistiche per le singole richieste e latenze del server Vscan

È possibile utilizzare ONTAP `offbox_vscan_server` Contatori su un server Vscan per-SVM, per-off-box, E per nodo per monitorare il tasso di richieste del server Vscan inviate e la latenza del server su Ciascun server Vscan singolarmente. Per raccogliere queste informazioni, completare la seguente fase:

Fase

1. Eseguire `statistics show -object offbox_vscan -instance SVM:servername:nodename` comando con i seguenti contatori:

Contatore…	Informazioni visualizzate…
`scan_request_dispatched_rate`	Numero di richieste di scansione virus inviate da ONTAP
`scan_latency`	Latenza di andata e ritorno da ONTAP al server Vscan, compreso il tempo di esecuzione della scansione Ai server Vscan al secondo

Esempio di statistiche generate da un contatore ONTAP offbox_vscan_server

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-----------------------------------------------------------------
```

Visualizzare le statistiche per l'utilizzo del server Vscan

È anche possibile utilizzare ONTAP `offbox_vscan_server` Contatori per raccogliere l'utilizzo del server Vscan
statistiche. Queste statistiche vengono monitorate per SVM, per server Vscan off-box e per nodo. Loro Includere l'utilizzo della CPU sul server Vscan, la profondità della coda per le operazioni di scansione sul server Vscan
(corrente e massima), memoria utilizzata e rete utilizzata.
Queste statistiche vengono inoltrate dal connettore antivirus ai contatori delle statistiche all'interno di ONTAP. Loro
sono basati su dati che vengono interrogati ogni 20 secondi e devono essere raccolti più volte per la precisione;
in caso contrario, i valori visualizzati nelle statistiche riflettono solo l'ultimo polling. L'utilizzo della CPU e le code sono
particolarmente importante per il monitoraggio e l'analisi. Un valore elevato per una coda media può indicare che
Il server Vscan presenta un collo di bottiglia.
Per raccogliere le statistiche di utilizzo per il server Vscan su un server Vscan per SVM, per server Vscan e per nodo
di base, completare il seguente passaggio:

Fase

1. Raccogliere le statistiche di utilizzo per il server Vscan

   Eseguire `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` con i seguenti comandi `offbox_vscan_server` contatori:

Contatore…	Informazioni visualizzate…
`scanner_stats_pct_cpu_used`	Utilizzo della CPU sul server Vscan
`scanner_stats_pct_input_queue_avg`	Coda media di richieste di scansione sul server Vscan
`scanner_stats_pct_input_queue_hiwatermark`	Coda di picco delle richieste di scansione sul server Vscan

`scanner_stats_pct_mem_used`	Memoria utilizzata sul server Vscan
`scanner_stats_pct_network_used`	Rete utilizzata sul server Vscan

Esempio di statistiche di utilizzo per il server Vscan

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
---------------------------------------------------------------
```

Audit degli eventi NAS su SVM

Controllo SMB e NFS e tracciamento della sicurezza

È possibile utilizzare le funzionalità di controllo dell'accesso ai file disponibili per i protocolli SMB e NFS con ONTAP, come il controllo nativo e la gestione dei criteri dei file utilizzando FPolicy.

È necessario progettare e implementare il controllo degli eventi di accesso ai file SMB e NFS nei seguenti casi:

- È stato configurato l'accesso di base ai file dei protocolli SMB e NFS.
- Si desidera creare e gestire una configurazione di controllo utilizzando uno dei seguenti metodi:
  - Funzionalità ONTAP nativa
  - Server FPolicy esterni

Audit degli eventi NAS su SVM

Il controllo degli eventi NAS è una misura di sicurezza che consente di tenere traccia e registrare determinati eventi SMB e NFS sulle macchine virtuali di storage (SVM). In questo modo è possibile tenere traccia dei potenziali problemi di sicurezza e fornire prove di eventuali violazioni della sicurezza. È inoltre possibile organizzare e controllare le policy di accesso centrale di Active Directory per verificare il risultato dell'implementazione.

Eventi SMB

È possibile controllare i seguenti eventi:

- Eventi di accesso a file e cartelle SMB

  È possibile controllare gli eventi di accesso a file e cartelle SMB sugli oggetti memorizzati nei volumi FlexVol appartenenti alle SVM abilitate per l'auditing.

- Eventi di logon e logoff SMB

  È possibile controllare gli eventi di logon e logoff SMB per i server SMB sulle SVM.

- Eventi di staging dei criteri di accesso centrale

  È possibile controllare l'accesso effettivo degli oggetti sui server SMB utilizzando le autorizzazioni applicate attraverso le policy di accesso centrale proposte. Il controllo attraverso lo staging delle policy di accesso centrale consente di verificare gli effetti delle policy di accesso centrale prima che vengano implementate.

  Il controllo dello staging dei criteri di accesso centrale viene impostato utilizzando gli oggetti Criteri di gruppo di Active Directory; tuttavia, la configurazione di controllo SVM deve essere configurata per controllare gli eventi di staging dei criteri di accesso centrale.

  Sebbene sia possibile attivare lo staging dei criteri di accesso centrale nella configurazione di controllo senza attivare il controllo dinamico degli accessi sul server SMB, gli eventi di staging dei criteri di accesso centrale vengono generati solo se è attivato il controllo dinamico degli accessi. Il controllo dinamico degli accessi viene attivato tramite un'opzione server SMB. Non è attivato per impostazione predefinita.

Eventi NFS

È possibile controllare gli eventi di file e directory utilizzando ACL NFSv4 sugli oggetti memorizzati sulle SVM.

Come funziona il controllo

Concetti di controllo di base

Per comprendere il controllo in ONTAP, è necessario conoscere alcuni concetti di base relativi al controllo.

- **File di staging**

  I file binari intermedi sui singoli nodi in cui vengono memorizzati i record di audit prima del consolidamento e della conversione. I file di staging sono contenuti nei volumi di staging.

- **Volume di staging**

  Un volume dedicato creato da ONTAP per memorizzare i file di staging. Esiste un volume di staging per aggregato. I volumi di staging sono condivisi da tutte le SVM (Storage Virtual Machine) abilitate all'audit per memorizzare i record di audit dell'accesso ai dati per i volumi di dati in quel particolare aggregato. I record di audit di ogni SVM sono memorizzati in una directory separata all'interno del volume di staging.

  Gli amministratori dei cluster possono visualizzare informazioni sui volumi di staging, ma la maggior parte delle altre operazioni sui volumi non è consentita. Solo ONTAP può creare volumi di staging. ONTAP assegna automaticamente un nome ai volumi di staging. Tutti i nomi dei volumi di staging iniziano con

`MDV_aud_` Seguito dall'UUID dell'aggregato contenente il volume di staging (ad esempio: `MDV_aud_1d0131843d4811e296fc123478563412`.)

- **Volumi di sistema**

  Volume FlexVol contenente metadati speciali, ad esempio metadati per i log di audit dei servizi file. La SVM amministrativa possiede i volumi di sistema, visibili all'interno del cluster. I volumi di staging sono un tipo di volume di sistema.

- **Attività di consolidamento**

  Un'attività che viene creata quando viene attivato il controllo. Questa attività a esecuzione prolungata su ogni SVM prende i record di audit dai file di staging attraverso i nodi membri della SVM. Questa attività unisce i record di audit in ordine cronologico ordinato, quindi li converte in un formato di registro eventi leggibile dall'utente specificato nella configurazione di controllo, ovvero IL formato DI file EVTX o XML. I registri eventi convertiti vengono memorizzati nella directory del registro eventi di controllo specificata nella configurazione di controllo SVM.

Come funziona il processo di audit di ONTAP

Il processo di controllo di ONTAP è diverso dal processo di controllo di Microsoft. Prima di configurare il controllo, è necessario comprendere il funzionamento del processo di controllo di ONTAP.

I record di audit vengono inizialmente memorizzati in file di staging binari su singoli nodi. Se il controllo è attivato su una SVM, ogni nodo membro mantiene i file di staging per tale SVM. Periodicamente, vengono consolidati e convertiti in registri eventi leggibili dall'utente, memorizzati nella directory del registro eventi di controllo per SVM.

Processo quando il controllo è attivato su una SVM

Il controllo può essere attivato solo sulle SVM. Quando l'amministratore dello storage abilita il controllo sulla SVM, il sottosistema di controllo verifica se sono presenti volumi di staging. Per ogni aggregato che contiene volumi di dati di proprietà di SVM deve esistere un volume di staging. Il sottosistema di auditing crea tutti i volumi di staging necessari, se non esistono.

Il sottosistema di auditing completa anche altre attività prerequisite prima che sia attivato il controllo:

- Il sottosistema di controllo verifica che il percorso della directory di log sia disponibile e non contenga symlink.

  La directory di log deve già esistere come percorso all'interno dello spazio dei nomi SVM. Si consiglia di creare un nuovo volume o qtree per contenere i file di log dell'audit. Il sottosistema di controllo non assegna una posizione predefinita per il file di log. Se il percorso della directory di log specificato nella configurazione di controllo non è un percorso valido, il controllo della creazione della configurazione non riesce con `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` errore.

  La creazione della configurazione non riesce se la directory esiste ma contiene collegamenti simbolici.

- Il controllo pianifica l'attività di consolidamento.

  Una volta pianificata questa attività, viene attivato il controllo. La configurazione di controllo SVM e i file di log rimangono durante un riavvio o se i server NFS o SMB vengono arrestati o riavviati.

Consolidamento del registro eventi

Il consolidamento dei log è un'attività pianificata che viene eseguita di routine fino alla disattivazione del controllo. Quando il controllo è disattivato, l'attività di consolidamento verifica che tutti i log rimanenti siano consolidati.

Auditing garantito

Per impostazione predefinita, il controllo è garantito. ONTAP garantisce la registrazione di tutti gli eventi di accesso ai file verificabili (come specificato dagli ACL dei criteri di controllo configurati), anche se un nodo non è disponibile. Un'operazione di file richiesta non può essere completata fino a quando il record di audit per tale operazione non viene salvato nel volume di staging sullo storage persistente. Se non è possibile eseguire il commit dei record di audit sul disco nei file di staging, a causa di spazio insufficiente o a causa di altri problemi, le operazioni del client vengono negate.

> Un amministratore, o un utente di account con accesso a livello di privilegio, può ignorare l'operazione di registrazione dell'audit del file utilizzando NetApp Manageability SDK o API REST. È possibile determinare se sono state eseguite azioni sui file utilizzando NetApp Manageability SDK o API REST esaminando i log della cronologia dei comandi memorizzati in `audit.log` file.
>
> Per ulteriori informazioni sui registri di audit della cronologia dei comandi, vedere la sezione "Gestione della registrazione dell'audit per le attività di gestione" in "Amministrazione del sistema".

Processo di consolidamento quando un nodo non è disponibile

Se un nodo contenente volumi appartenenti a una SVM con il controllo attivato non è disponibile, il comportamento dell'attività di consolidamento del controllo dipende dalla disponibilità del partner di storage failover (SFO) del nodo (o del partner ha nel caso di un cluster a due nodi):

- Se il volume di staging è disponibile tramite il partner SFO, l'ultima scansione dei volumi di staging segnalati dal nodo viene eseguita e il consolidamento procede normalmente.
- Se il partner SFO non è disponibile, l'attività crea un file di log parziale.

  Quando un nodo non è raggiungibile, l'attività di consolidamento consolida i record di audit degli altri nodi disponibili di tale SVM. Per identificare che non è completo, l'attività aggiunge il suffisso `.partial` al nome del file consolidato.

- Una volta disponibile il nodo non disponibile, i record di audit in quel nodo vengono consolidati con i record di audit degli altri nodi in quel momento.
- Tutti i record di audit vengono conservati.

Rotazione del registro eventi

I file di log degli eventi di audit vengono ruotati quando raggiungono una dimensione di log di soglia configurata o in base a una pianificazione configurata. Quando un file di registro eventi viene ruotato, l'attività di consolidamento pianificata rinomina prima il file convertito attivo in un file di archivio con data e ora, quindi crea un nuovo file di registro eventi convertito attivo.

Processo quando il controllo è disattivato su SVM

Quando il controllo viene disattivato sulla SVM, l'attività di consolidamento viene attivata una volta finale. Tutti i record di audit registrati in sospeso vengono registrati in un formato leggibile dall'utente. I registri eventi

esistenti memorizzati nella directory del registro eventi non vengono cancellati quando il controllo viene disattivato sulla SVM e sono disponibili per la visualizzazione.

Una volta consolidati tutti i file di staging esistenti per la SVM, l'attività di consolidamento viene rimossa dalla pianificazione. La disattivazione della configurazione di controllo per SVM non rimuove la configurazione di controllo. Un amministratore dello storage può riabilitare il controllo in qualsiasi momento.

Il processo di consolidamento di controllo, creato quando viene attivato il controllo, monitora l'attività di consolidamento e la ricrea se l'attività di consolidamento viene chiusa a causa di un errore. Gli utenti non possono eliminare il processo di consolidamento del controllo.

Requisiti e considerazioni per il controllo

Prima di configurare e abilitare l'auditing sulla macchina virtuale di storage (SVM), è necessario essere a conoscenza di determinati requisiti e considerazioni.

- Il numero massimo di SVM abilitate all'audit supportate dipende dalla versione di ONTAP in uso:

Versione di ONTAP	Massimo
9,8 e precedenti	50
9.9.1 e versioni successive	400

- Il controllo non è legato alle licenze SMB o NFS.

  È possibile configurare e abilitare il controllo anche se le licenze SMB e NFS non sono installate nel cluster.

- Il controllo NFS supporta ACE di sicurezza (tipo U).
- Per il controllo NFS, non esiste alcuna mappatura tra i bit di modalità e le ACE di controllo.

  Quando si convertono gli ACL in bit di modalità, gli ACE di controllo vengono ignorati. Quando si convertono i bit di modalità in ACL, non vengono generati ACE di controllo.

- La directory specificata nella configurazione di controllo deve esistere.

  Se non esiste, il comando per creare la configurazione di controllo non riesce.

- La directory specificata nella configurazione di controllo deve soddisfare i seguenti requisiti:
  - La directory non deve contenere collegamenti simbolici.

    Se la directory specificata nella configurazione di controllo contiene collegamenti simbolici, il comando per creare la configurazione di controllo non riesce.

  - Specificare la directory utilizzando un percorso assoluto.

    Non specificare un percorso relativo, ad esempio `/vs1/../`.

- Il controllo dipende dalla disponibilità di spazio nei volumi di staging.

  È necessario conoscere e disporre di un piano per garantire che vi sia spazio sufficiente per i volumi di staging negli aggregati che contengono volumi sottoposti a audit.

- Il controllo dipende dalla disponibilità di spazio nel volume contenente la directory in cui sono memorizzati i registri degli eventi convertiti.

  È necessario conoscere e disporre di un piano per garantire che vi sia spazio sufficiente nei volumi utilizzati per memorizzare i registri degli eventi. È possibile specificare il numero di registri eventi da conservare nella directory di controllo utilizzando `-rotate-limit` parametro durante la creazione di una configurazione di controllo, che può aiutare a garantire che vi sia spazio disponibile sufficiente per i registri degli eventi nel volume.

- Sebbene sia possibile attivare lo staging dei criteri di accesso centrale nella configurazione di controllo senza attivare il controllo dinamico degli accessi sul server SMB, il controllo dinamico degli accessi deve essere abilitato per generare eventi di staging dei criteri di accesso centrale.

  Dynamic Access Control non è attivato per impostazione predefinita.

Aggregare le considerazioni sullo spazio quando si abilita il controllo

Quando viene creata una configurazione di audit e viene attivato il controllo su almeno una macchina virtuale di storage (SVM) nel cluster, il sottosistema di audit crea volumi di staging su tutti gli aggregati esistenti e su tutti i nuovi aggregati creati. Quando si abilita il controllo sul cluster, è necessario tenere conto di alcune considerazioni relative allo spazio aggregato.

La creazione del volume di staging potrebbe non riuscire a causa della non disponibilità di spazio in un aggregato. Questo potrebbe verificarsi se si crea una configurazione di controllo e gli aggregati esistenti non dispongono di spazio sufficiente per contenere il volume di staging.

Prima di attivare il controllo su una SVM, è necessario assicurarsi che vi sia spazio sufficiente sugli aggregati esistenti per i volumi di staging.

Limiti per la dimensione dei record di audit sui file di staging

La dimensione di un record di audit in un file di staging non può essere superiore a 32 KB.

Quando possono verificarsi record di audit di grandi dimensioni

Durante il controllo della gestione potrebbero verificarsi record di audit di grandi dimensioni in uno dei seguenti scenari:

- Aggiunta o eliminazione di utenti a o da gruppi con un elevato numero di utenti.
- Aggiunta o eliminazione di un elenco di controllo di accesso (ACL) per la condivisione di file con un gran numero di utenti per la condivisione di file.
- Altri scenari.

Disattivare il controllo di gestione per evitare questo problema. A tale scopo, modificare la configurazione dell'audit e rimuovere quanto segue dall'elenco dei tipi di eventi di audit:

- condivisione file
- account utente
- security-group
- authorization-policy-change

Dopo la rimozione, non verranno controllati dal sottosistema di controllo dei file Services.

Gli effetti di record di audit troppo grandi

- Se la dimensione di un record di audit è troppo grande (oltre 32 KB), il record di audit non viene creato e il sottosistema di audit genera un messaggio EMS (Event Management System) simile a quanto segue:

  ```
  File Services Auditing subsystem failed the operation or truncated an audit
  record because it was greater than max_audit_record_size value. Vserver
  UUID=%s, event_id=%u, size=%u
  ```

  Se il controllo è garantito, l'operazione del file non riesce perché non è possibile creare il relativo record di audit.

- Se la dimensione del record di audit è superiore a 9,999 byte, viene visualizzato lo stesso messaggio EMS riportato sopra. Viene creato un record di audit parziale con il valore chiave più grande mancante.
- Se il record di audit supera i 2,000 caratteri, viene visualizzato il seguente messaggio di errore anziché il valore effettivo:

  ```
  The value of this field was too long to display.
  ```

Quali sono i formati di registro eventi di audit supportati

I formati di file supportati per i registri degli eventi di audit convertiti sono `EVTX` e. `XML` formati di file.

È possibile specificare il tipo di formato del file quando si crea la configurazione di controllo. Per impostazione predefinita, ONTAP converte i registri binari in `EVTX` formato del file.

Visualizzare i registri degli eventi di audit

È possibile utilizzare i registri degli eventi di audit per determinare se si dispone di una protezione dei file adeguata e se si sono verificati tentativi di accesso a file e cartelle non corretti. È possibile visualizzare ed elaborare i registri degli eventi di audit salvati in `EVTX` oppure `XML` formati di file.

- `EVTX` formato del file

  È possibile aprire il file convertito `EVTX` Controllare i log degli eventi come file salvati utilizzando Microsoft Event Viewer.

  È possibile utilizzare due opzioni per la visualizzazione dei registri eventi mediante il Visualizzatore eventi:

  - Vista generale

    Le informazioni comuni a tutti gli eventi vengono visualizzate per il record dell'evento. In questa versione di ONTAP, i dati specifici dell'evento per il record dell'evento non vengono visualizzati. È possibile utilizzare la vista dettagliata per visualizzare i dati specifici dell'evento.

  - Vista dettagliata

Sono disponibili una vista intuitiva e una vista XML. La visualizzazione semplice e la visualizzazione XML visualizzano sia le informazioni comuni a tutti gli eventi che i dati specifici dell'evento per il record dell'evento.

- `XML` formato del file

  È possibile visualizzare ed elaborare `XML` registri degli eventi di audit su applicazioni di terze parti che supportano `XML` formato del file. È possibile utilizzare gli strumenti di visualizzazione XML per visualizzare i registri di controllo, a condizione che si disponga dello schema XML e delle informazioni sulle definizioni dei campi XML. Per ulteriori informazioni sullo schema e sulle definizioni XML, vedere "Riferimento allo schema di controllo ONTAP".

Visualizzazione dei registri di controllo attivi mediante Event Viewer

Se il processo di consolidamento dell'audit è in esecuzione sul cluster, il processo di consolidamento aggiunge nuovi record al file di log dell'audit attivo per le macchine virtuali dello storage abilitate all'audit (SVM). È possibile accedere a questo registro di controllo attivo e aprirlo tramite una condivisione SMB in Microsoft Event Viewer.

Oltre a visualizzare i record di audit esistenti, Event Viewer offre un'opzione di refresh che consente di aggiornare il contenuto nella finestra della console. La possibilità di visualizzare i nuovi registri aggiunti nel Visualizzatore eventi dipende dall'attivazione o meno degli oplock nella condivisione utilizzata per accedere al registro di controllo attivo.

Impostazione degli oplock sulla condivisione	Comportamento
Attivato	Event Viewer apre il registro contenente gli eventi scritti fino a quel momento. L'operazione di refresh non aggiorna il log con nuovi eventi aggiunti dal processo di consolidamento.
Disattivato	Event Viewer apre il registro contenente gli eventi scritti fino a quel momento. L'operazione di refresh aggiorna il log con nuovi eventi aggiunti dal processo di consolidamento.

Queste informazioni sono valide solo per `EVTX` registri eventi. `XML` I registri degli eventi possono essere visualizzati tramite SMB in un browser o NFS utilizzando qualsiasi editor o visualizzatore XML.

Eventi SMB che possono essere verificati

Panoramica degli eventi SMB che è possibile verificare

ONTAP può controllare alcuni eventi SMB, inclusi determinati eventi di accesso a file e cartelle, determinati eventi di accesso e disconnessione ed eventi di staging dei criteri di accesso centrale. Sapere quali eventi di accesso è possibile verificare è utile quando si interpretano i risultati dei registri eventi.

I seguenti eventi SMB aggiuntivi possono essere verificati in ONTAP 9.2 e versioni successive:

ID EVENTO (EVT/EVTX)	Evento	Descrizione	Categoria
4670	Le autorizzazioni degli oggetti sono state modificate	OBJECT ACCESS (ACCESSO A OGGETTI): Autorizzazioni modificate.	Accesso al file
4907	Le impostazioni di controllo degli oggetti sono state modificate	OBJECT ACCESS (ACCESSO A OGGETTI): Impostazioni di controllo modificate.	Accesso al file
4913	La policy di accesso di Object Central è stata modificata	ACCESSO A OGGETTI: CAP MODIFICATO.	Accesso al file

I seguenti eventi SMB possono essere verificati in ONTAP 9.0 e versioni successive:

ID EVENTO (EVT/EVTX)	Evento	Descrizione	Categoria
540/4624	Un account è stato collegato correttamente	LOGON/LOGOFF: Accesso alla rete (SMB).	Accesso e disconnessione
529/4625	Impossibile accedere a un account	LOGON/LOGOFF: Nome utente sconosciuto o password errata.	Accesso e disconnessione
530/4625	Impossibile accedere a un account	LOGON/LOGOFF: Limite di tempo per l'accesso all'account.	Accesso e disconnessione
531/4625	Impossibile accedere a un account	LOGON/LOGOFF: Account attualmente disattivato.	Accesso e disconnessione
532/4625	Impossibile accedere a un account	LOGON/LOGOFF: L'account utente è scaduto.	Accesso e disconnessione
533/4625	Impossibile accedere a un account	LOGON/LOGOFF (ACCESSO/DISCONNESSIONE): L'utente non può accedere al computer.	Accesso e disconnessione
534/4625	Impossibile accedere a un account	LOGON/LOGOFF: L'utente non ha concesso il tipo di accesso qui.	Accesso e disconnessione
535/4625	Impossibile accedere a un account	LOGON/LOGOFF: La password dell'utente è scaduta.	Accesso e disconnessione
537/4625	Impossibile accedere a un account	LOGON/LOGOFF: Accesso non riuscito per motivi diversi da quelli sopra indicati.	Accesso e disconnessione

539/4625	Impossibile accedere a un account	LOGON/LOGOFF: Account bloccato.	Accesso e disconnessione
538/4634	Un account è stato disconnesso	LOGON/LOGOFF: Disconnessione dell'utente locale o di rete.	Accesso e disconnessione
560/4656	Apri oggetto/Crea oggetto	ACCESSO A OGGETTI: Oggetto (file o directory) aperto.	Accesso al file
563/4659	Aprire l'oggetto con l'intento di eliminare	ACCESSO A OGGETTI: È stato richiesto un handle a un oggetto (file o directory) con l'intento di eliminare.	Accesso al file
564/4660	Elimina oggetto	OBJECT ACCESS (ACCESSO A OGGETTI): Elimina oggetto (file o directory). ONTAP genera questo evento quando un client Windows tenta di eliminare l'oggetto (file o directory).	Accesso al file
567/4663	Read Object/Write Object/Get Object Attributes/Set Object Attributes	ACCESSO A OGGETTI: Tentativo di accesso a oggetti (lettura, scrittura, attributo get, attributo set). **Nota:** per questo evento, ONTAP controlla solo la prima operazione di lettura SMB e la prima operazione di scrittura SMB (successo o errore) su un oggetto. Ciò impedisce a ONTAP di creare voci di registro eccessive quando un singolo client apre un oggetto ed esegue molte operazioni di lettura o scrittura successive sullo stesso oggetto.	Accesso al file
NA/4664	Collegamento rigido	OBJECT ACCESS (ACCESSO A OGGETTI): Tentativo di creazione di un hard link.	Accesso al file
NA/4818	Il criterio di accesso centrale proposto non concede le stesse autorizzazioni di accesso del criterio di accesso centrale corrente	ACCESSO A OGGETTI: Gestione temporanea dei criteri di accesso centrale.	Accesso al file

ID evento Data ONTAP NA/NA 9999	Rinominare l'oggetto	ACCESSO AGLI OGGETTI: Oggetto rinominato. Si tratta di un evento ONTAP. Attualmente non è supportato da Windows come singolo evento.	Accesso al file
ID evento Data ONTAP NA/NA 9998	Scollegare l'oggetto	ACCESSO A OGGETTI: Oggetto non collegato. Si tratta di un evento ONTAP. Attualmente non è supportato da Windows come singolo evento.	Accesso al file

Ulteriori informazioni sull'evento 4656

Il `HandleID` tag nell'audit `XML` l'evento contiene l'handle dell'oggetto (file o directory) a cui si accede. Il `HandleID` Tag per L'evento EVTX 4656 contiene informazioni diverse a seconda che l'evento aperto sia per la creazione di un nuovo oggetto o per l'apertura di un oggetto esistente:

- Se l'evento open è una richiesta di apertura per creare un nuovo oggetto (file o directory), il `HandleID` Il tag nell'evento XML di audit mostra un valore vuoto `HandleID` (ad esempio: `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`).

  Il `HandleID` È vuoto perché la richiesta DI APERTURA (per la creazione di un nuovo oggetto) viene controllata prima che avvenga la creazione effettiva dell'oggetto e prima che esista un handle. Gli eventi controllati successivi per lo stesso oggetto hanno il giusto handle di oggetto in `HandleID` tag.

- Se l'evento open è una richiesta aperta per aprire un oggetto esistente, l'evento di audit avrà l'handle assegnato di tale oggetto in `HandleID` tag (ad esempio: `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`).

Determinare il percorso completo dell'oggetto verificato

Il percorso dell'oggetto stampato in `<ObjectName>` il tag per un record di audit contiene il nome del volume (tra parentesi) e il percorso relativo dalla directory principale del volume contenente. Se si desidera determinare il percorso completo dell'oggetto sottoposto a audit, incluso il percorso di giunzione, è necessario eseguire alcuni passaggi.

Fasi

1. Determinare il nome del volume e il relativo percorso dell'oggetto sottoposto a controllo osservando il `<ObjectName>` tag nell'evento di audit.

   In questo esempio, il nome del volume è "data1" e il percorso relativo al file è `/dir1/file.txt`:

   ```
   <Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
   ```

2. Utilizzando il nome del volume determinato nella fase precedente, determinare il percorso di giunzione per il volume contenente l'oggetto verificato:

   In questo esempio, il nome del volume è "data1" e il percorso di giunzione per il volume contenente

l'oggetto sottoposto a audit è `/data/data1`:

```
volume show -junction -volume data1
```

```
                                Junction                     Junction
Vserver   Volume       Language Active    Junction Path     Path Source
--------- ------------ -------- --------  ----------------- -----------
vs1       data1        en_US.UTF-8
                                true      /data/data1       RW_volume
```

3. Determinare il percorso completo dell'oggetto verificato aggiungendo il percorso relativo trovato in `<ObjectName>` contrassegnare il percorso di giunzione per il volume.

   In questo esempio, il percorso di giunzione per il volume:

   ```
   /data/data1/dir1/file.text
   ```

Considerazioni per il controllo di collegamenti simbolici e hard link

Ci sono alcune considerazioni da tenere a mente quando si esegue il controllo dei collegamenti simbolici e dei collegamenti rigidi.

Un record di audit contiene informazioni sull'oggetto sottoposto a audit, incluso il percorso dell'oggetto sottoposto a audit, identificato in `ObjectName` tag. È necessario conoscere come vengono registrati i percorsi per i collegamenti simbolici e gli hard link in `ObjectName` tag.

Link simbolici

Un collegamento simbolico è un file con un inode separato che contiene un puntatore alla posizione di un oggetto di destinazione, noto come destinazione. Quando si accede a un oggetto tramite un collegamento simbolico, ONTAP interpreta automaticamente il collegamento simbolico e segue il percorso indipendente dal protocollo canonico effettivo verso l'oggetto di destinazione nel volume.

Nell'output dell'esempio seguente, sono presenti due collegamenti simbolici, entrambi rivolti a un file denominato `target.txt`. Uno dei link simbolici è un link simbolico relativo e uno è un link simbolico assoluto. Se uno dei collegamenti simbolici viene controllato, il `ObjectName` tag nell'evento di audit contiene il percorso del file `target.txt`:

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

Collegamenti hardware

Un hard link è una voce di directory che associa un nome a un file esistente su un file system. L'hard link punta

alla posizione inode del file originale. Analogamente a quanto ONTAP interpreta i collegamenti simbolici, ONTAP interpreta il collegamento rigido e segue il percorso canonico effettivo dell'oggetto di destinazione nel volume. Quando viene verificato l'accesso a un oggetto hard link, l'evento di audit registra questo percorso canonico assoluto in `ObjectName` piuttosto che il percorso hard link.

Considerazioni per il controllo di flussi di dati NTFS alternativi

È necessario tenere presente alcune considerazioni durante il controllo dei file con flussi di dati alternativi NTFS.

La posizione di un oggetto sottoposto a audit viene registrata in un record di evento utilizzando due tag, l' `ObjectName` tag (il percorso) e il `HandleID` tag (l'impugnatura). Per identificare correttamente le richieste di flusso registrate, è necessario conoscere i record ONTAP presenti in questi campi per i flussi di dati alternativi NTFS:

- ID EVTX: 4656 eventi (aprire e creare eventi di audit)
  - Il percorso del flusso di dati alternativo viene registrato in `ObjectName` tag.
  - L'handle del flusso di dati alternativo viene registrato in `HandleID` tag.
- ID EVTX: 4663 eventi (tutti gli altri eventi di audit, come lettura, scrittura, getattr e così via)
  - Il percorso del file di base, non del flusso di dati alternativo, viene registrato in `ObjectName` tag.
  - L'handle del flusso di dati alternativo viene registrato in `HandleID` tag.

Esempio

Nell'esempio seguente viene illustrato come identificare L'ID EVTX: 4663 eventi per flussi di dati alternativi che utilizzano `HandleID` tag. Anche se il `ObjectName` il tag (percorso) registrato nell'evento di controllo in lettura si trova nel percorso del file di base, il `HandleID` il tag può essere utilizzato per identificare l'evento come record di audit per il flusso di dati alternativo.

I nomi dei file di streaming hanno la forma `base_file_name:stream_name`. In questo esempio, il `dir1` la directory contiene un file di base con un flusso di dati alternativo con i seguenti percorsi:

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

> L'output nel seguente esempio di evento viene troncato come indicato; l'output non visualizza tutti i tag di output disponibili per gli eventi.

Per un ID EVTX 4656 (evento di audit aperto), l'output del record di audit per il flusso di dati alternativo registra il nome del flusso di dati alternativo in `ObjectName` tag:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

Per un ID EVTX 4663 (evento di audit in lettura), l'output del record di audit per lo stesso flusso di dati alternativo registra il nome del file di base in `ObjectName` tag; tuttavia, l'handle in `HandleID` tag è l'handle alternativo del flusso di dati e può essere utilizzato per correlare questo evento con il flusso di dati alternativo:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

Eventi di accesso a file e directory NFS che possono essere controllati

ONTAP può controllare alcuni eventi di accesso a file e directory NFS. Sapere quali eventi di accesso possono essere verificati è utile quando si interpretano i risultati dei registri degli eventi di audit convertiti.

È possibile controllare i seguenti eventi di accesso a file e directory NFS:

- LEGGI
- APRIRE
- CHIUDERE
- READDIR
- DI SCRITTURA
- SETATTR
- CREARE
- COLLEGAMENTO
- OPENATTR
- RIMUOVERE
- GETATTR
- VERIFICARE
- NVERIFICARE
- RINOMINARE

Per controllare in modo affidabile gli eventi DI RIDENOMINAZIONE NFS, è necessario impostare ACE di controllo sulle directory invece che sui file, in quanto le autorizzazioni dei file non vengono controllate per un'operazione DI RIDENOMINAZIONE, se le autorizzazioni della directory sono sufficienti.

Pianificare la configurazione di controllo

Prima di configurare il controllo sulle macchine virtuali di storage, è necessario comprendere quali opzioni di configurazione sono disponibili e pianificare i valori che si desidera impostare per ciascuna opzione. Queste informazioni possono aiutarti a configurare la configurazione di controllo che soddisfa le tue esigenze di business.

Alcuni parametri di configurazione sono comuni a tutte le configurazioni di controllo.

Inoltre, è possibile utilizzare alcuni parametri per specificare i metodi da utilizzare durante la rotazione dei registri di controllo consolidati e convertiti. Quando si configura il controllo, è possibile specificare uno dei tre metodi seguenti:

- Ruotare i registri in base alle dimensioni del registro

  Questo è il metodo predefinito utilizzato per ruotare i registri.

- Ruotare i registri in base a una pianificazione
- Rotazione dei registri in base alle dimensioni e alla pianificazione del registro (a seconda dell'evento che si verifica per primo)
  F

È necessario impostare almeno uno dei metodi per la rotazione del log.

Parametri comuni a tutte le configurazioni di controllo

Sono necessari due parametri da specificare quando si crea la configurazione di controllo. Sono inoltre disponibili tre parametri opzionali che è possibile specificare:

Tipo di informazione	Opzione	Obbligatorio	Includi	I tuoi valori
Nome SVM Nome della SVM su cui creare la configurazione di controllo. La SVM deve già esistere.	`-vserver vserver_name`	Sì	Sì	
Percorso di destinazione del registro Specifica la directory in cui sono memorizzati i log di audit convertiti, in genere un volume dedicato o un qtree. Il percorso deve già esistere nello spazio dei nomi SVM. Il percorso può contenere fino a 864 caratteri e deve disporre di permessi di lettura/scrittura. Se il percorso non è valido, il comando di configurazione del controllo non riesce. Se SVM è un'origine di disaster recovery SVM, il percorso di destinazione del log non può trovarsi sul volume root. Questo perché il contenuto del volume root non viene replicato nella destinazione del disaster recovery. Non è possibile utilizzare un volume FlexCache come destinazione del registro (ONTAP 9.7 e versioni successive).	`-destination text`	Sì	Sì	

Categorie di eventi da controllare Specifica le categorie di eventi da controllare. È possibile verificare le seguenti categorie di eventi: • Eventi di accesso al file (SMB e NFSv4) • Eventi di logon e logoff SMB • Eventi di staging dei criteri di accesso centrale Gli eventi di staging dei criteri di accesso centrale sono disponibili a partire dai domini Active Directory di Windows 2012. • Eventi categoria condivisione file • Eventi di modifica delle policy di audit • Eventi di gestione dell'account utente locale • Eventi di gestione dei gruppi di sicurezza • Eventi di modifica del criterio di autorizzazione Per impostazione predefinita, viene eseguito il controllo dell'accesso al file e degli eventi di logon e logoff SMB. **Nota:** prima di poter specificare `cap-staging` Come categoria di evento, un server SMB deve esistere sulla SVM. Sebbene sia possibile attivare lo staging dei criteri di accesso centrale nella configurazione di controllo senza attivare il controllo dinamico degli accessi sul server SMB, gli eventi di staging dei criteri di accesso centrale vengono generati solo se è attivato il controllo dinamico degli accessi. Il controllo dinamico degli accessi viene attivato tramite un'opzione server SMB. Non è attivato per impostazione predefinita.	`-events` {`file-ops`	`cifs-logon-logoff`	`cap-staging`	`file-share`
`audit-policy-change`	`user-account`	`security-group`	`authorization-policy-change`}	No

		Formato di output del file di log Determina il formato di output dei registri di controllo. Il formato di output può essere specifico di ONTAP `XML` O Microsoft Windows `EVTX` formato del log. Per impostazione predefinita, il formato di output è `EVTX`.	`-format` {`xml`	`evtx`}

No			*Limite di rotazione dei file di log* Determina il numero di file di log di audit da conservare prima di estrarre il file di log più vecchio. Ad esempio, se si immette un valore di `5`, vengono conservati gli ultimi cinque file di log. Un valore di `0` indica che tutti i file di log vengono conservati. Il valore predefinito è 0.	`-rotate-limit integer`

Parametri utilizzati per determinare quando ruotare i registri degli eventi di audit

Ruota i registri in base alle dimensioni del registro

L'impostazione predefinita prevede la rotazione dei registri di controllo in base alle dimensioni.

- La dimensione predefinita del registro è 100 MB
- Se si desidera utilizzare il metodo di rotazione del log predefinito e la dimensione del log predefinita, non è necessario configurare alcun parametro specifico per la rotazione del log.
- Se si desidera ruotare i registri di controllo solo in base alle dimensioni del registro, utilizzare il comando seguente per annullare l'impostazione di `-rotate-schedule-minute` parametro: `vserver audit`

```
modify -vserver vs0 -destination / -rotate-schedule-minute -
```

Se non si desidera utilizzare la dimensione predefinita del registro, è possibile configurare `-rotate-size` parametro per specificare una dimensione di log personalizzata:

Tipo di informazione	Opzione	Obbligatorio	Includi	I tuoi valori
Limite dimensioni file di log Determina il limite delle dimensioni del file di log di audit.	`-rotate-size` {`integer`[KB	MB	GB	TB

Rotazione dei registri in base a una pianificazione

Se si sceglie di ruotare i registri di controllo in base a una pianificazione, è possibile pianificare la rotazione dei registri utilizzando i parametri di rotazione basati sul tempo in qualsiasi combinazione.

- Se si utilizza la rotazione basata sul tempo, il `-rotate-schedule-minute` il parametro è obbligatorio.
- Tutti gli altri parametri di rotazione basati sul tempo sono opzionali.
- Il programma di rotazione viene calcolato utilizzando tutti i valori relativi al tempo.

  Ad esempio, se si specifica solo il `-rotate-schedule-minute` i file di log di audit vengono ruotati in base ai minuti specificati in tutti i giorni della settimana, durante tutte le ore in tutti i mesi dell'anno.

- Se si specificano solo uno o due parametri di rotazione basati sul tempo (ad esempio, `-rotate -schedule-month` e. `-rotate-schedule-minutes`), i file di log vengono ruotati in base ai valori dei minuti specificati in tutti i giorni della settimana, durante tutte le ore, ma solo durante i mesi specificati.

  Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato durante i mesi di gennaio, marzo e agosto tutti i lunedì, mercoledì e sabato alle 10:30

- Se si specificano i valori per entrambi `-rotate-schedule-dayofweek` e. `-rotate-schedule-day`, sono considerati indipendenti.

  Ad esempio, se si specifica `-rotate-schedule-dayofweek` Come venerdì e. `-rotate-schedule -day` Come 13, i registri di audit verrebbero ruotati ogni venerdì e il 13° giorno del mese specificato, non solo ogni venerdì 13.

- Se si desidera ruotare i registri di controllo solo in base a una pianificazione, utilizzare il comando seguente per annullare l'impostazione di `-rotate-size` parametro: `vserver audit modify -vserver vs0 -destination / -rotate-size -`

È possibile utilizzare il seguente elenco di parametri di controllo disponibili per determinare i valori da utilizzare per la configurazione di una pianificazione per le rotazioni del registro eventi di controllo:

Tipo di informazione	Opzione	Obbligatorio	Includi	I tuoi valori

Programma di rotazione del log: Mese Determina la pianificazione mensile per la rotazione dei registri di audit. I valori validi sono `January` attraverso `December`, e. `all`. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato nei mesi di gennaio, marzo e agosto.	`-rotate-schedule-month chron_month`	No		
Programma di rotazione del log: Giorno della settimana Determina la pianificazione giornaliera (giorno della settimana) per la rotazione dei registri di audit. I valori validi sono `Sunday` attraverso `Saturday`, e. `all`. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato il martedì e il venerdì o durante tutti i giorni di una settimana.	`-rotate-schedule -dayofweek chron_dayofweek`	No		
Programma di rotazione del log: Giorno Determina il giorno della pianificazione del mese per la rotazione del registro di audit. I valori validi sono compresi tra `1` attraverso `31`. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato il 10° e il 20° giorno di un mese o tutti i giorni di un mese.	`-rotate-schedule-day chron_dayofmonth`	No		
Programma di rotazione del log: Ora Determina la pianificazione oraria per la rotazione del registro di audit. I valori validi sono compresi tra `0` (mezzanotte) a. `23` (11:00). Specificare `all` ruota i registri di controllo ogni ora. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato alle 6 (6:00) e alle 18 (18:00).	`-rotate-schedule-hour chron_hour`	No		

Log Rotation schedule: Minute Determina la pianificazione dei minuti per la rotazione del registro di controllo. I valori validi sono compresi tra `0` a. `59`. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato al 30° minuto.	`-rotate-schedule-minute` `chron_minute`	Sì, se si configura la rotazione del log in base alla pianificazione; in caso contrario, no		

Rotazione dei registri in base alle dimensioni e alla pianificazione dei registri

È possibile scegliere di ruotare i file di log in base alle dimensioni e alla pianificazione del log impostando entrambi i campi `-rotate-size` e i parametri di rotazione basati sul tempo in qualsiasi combinazione. Ad esempio: Se `-rotate-size` È impostato su 10 MB e. `-rotate-schedule-minute` È impostato su 15, i file di log ruotano quando le dimensioni del file di log raggiungono i 10 MB o al 15° minuto di ogni ora (a seconda dell'evento che si verifica per primo).

Creare una configurazione di controllo di file e directory sulle SVM

Creare la configurazione di controllo

La creazione di una configurazione per il controllo di file e directory sulla macchina virtuale di storage (SVM) include la comprensione delle opzioni di configurazione disponibili, la pianificazione della configurazione, quindi la configurazione e l'abilitazione della configurazione. È quindi possibile visualizzare le informazioni sulla configurazione di controllo per confermare che la configurazione risultante è quella desiderata.

Prima di iniziare il controllo degli eventi di file e directory, è necessario creare una configurazione di controllo sulla macchina virtuale di storage (SVM).

Prima di iniziare

Se si prevede di creare una configurazione di controllo per lo staging dei criteri di accesso centrale, è necessario che un server SMB esista sulla SVM.

- Sebbene sia possibile attivare lo staging dei criteri di accesso centrale nella configurazione di controllo senza attivare il controllo dinamico degli accessi sul server SMB, gli eventi di staging dei criteri di accesso centrale vengono generati solo se è attivato il controllo dinamico degli accessi.

  Il controllo dinamico degli accessi viene attivato tramite un'opzione server SMB. Non è attivato per impostazione predefinita.

- Se gli argomenti di un campo in un comando non sono validi, ad esempio voci non valide per campi, voci duplicate e voci non esistenti, il comando non riesce prima della fase di audit.

  Tali errori non generano un record di audit.

A proposito di questa attività

Se SVM è un'origine di disaster recovery SVM, il percorso di destinazione non può trovarsi sul volume root.

Fase

1. Utilizzando le informazioni contenute nel foglio di lavoro di pianificazione, creare la configurazione di controllo per ruotare i registri di controllo in base alle dimensioni del log o a una pianificazione:

Se si desidera ruotare i registri di audit di…	Inserisci…
Dimensione del log	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
Un calendario	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

Esempi

Nell'esempio seguente viene creata una configurazione di controllo che controlla le operazioni dei file e gli eventi di logon e logoff SMB (impostazione predefinita) utilizzando la rotazione basata sulle dimensioni. Il formato del log è `EVTX` (impostazione predefinita). I registri vengono memorizzati in `/audit_log` directory. Il limite delle dimensioni del file di registro è `200 MB`. I log vengono ruotati quando raggiungono le dimensioni di 200 MB:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

Nell'esempio seguente viene creata una configurazione di controllo che controlla le operazioni dei file e gli eventi di logon e logoff SMB (impostazione predefinita) utilizzando la rotazione basata sulle dimensioni. Il formato del log è `EVTX` (impostazione predefinita). I registri vengono memorizzati in `/cifs_event_logs` directory. Il limite delle dimensioni del file di registro è `100 MB` (l'impostazione predefinita) e il limite di rotazione del registro è `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

Nell'esempio seguente viene creata una configurazione di controllo che controlla le operazioni dei file, gli

eventi di logon e logoff di CIFS e gli eventi di staging dei criteri di accesso centrale utilizzando la rotazione basata sul tempo. Il formato del log è `EVTX` (impostazione predefinita). I registri di audit vengono ruotati mensilmente alle 12:30 tutti i giorni della settimana. Il limite di rotazione del log è `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

Abilitare il controllo su SVM

Una volta completata l'impostazione della configurazione di controllo, è necessario attivare il controllo sulla macchina virtuale di storage (SVM).

Di cosa hai bisogno

La configurazione dell'audit SVM deve già esistere.

A proposito di questa attività

Quando una configurazione di eliminazione dell'ID di disaster recovery SVM viene avviata per la prima volta (dopo il completamento dell'inizializzazione di SnapMirror) e la SVM dispone di una configurazione di controllo, ONTAP disattiva automaticamente la configurazione di controllo. Il controllo viene disattivato sulla SVM di sola lettura per impedire il riempimento dei volumi di staging. È possibile attivare il controllo solo dopo che la relazione SnapMirror è stata interrotta e la SVM è in lettura/scrittura.

Fase

1. Abilitare il controllo su SVM:

   ```
   vserver audit enable -vserver vserver_name
   ```

   ```
   vserver audit enable -vserver vs1
   ```

Verificare la configurazione di controllo

Dopo aver completato la configurazione di controllo, verificare che il controllo sia configurato correttamente e che sia attivato.

Fasi

1. Verificare la configurazione di controllo:

   ```
   vserver audit show -instance -vserver vserver_name
   ```

   Il seguente comando visualizza sotto forma di elenco tutte le informazioni di controllo della configurazione per la macchina virtuale di storage (SVM) vs1:

   ```
   vserver audit show -instance -vserver vs1
   ```

```
                            Vserver: vs1
                     Auditing state: true
               Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops
                         Log Format: evtx
                 Log File Size Limit: 200MB
       Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
       Log Rotation Schedule: Hour: -
     Log Rotation Schedule: Minute: -
                 Rotation Schedules: -
           Log Files Rotation Limit: 0
```

Configurare i criteri di controllo di file e cartelle

Configurare i criteri di controllo di file e cartelle

L'implementazione del controllo sugli eventi di accesso a file e cartelle è un processo in due fasi. Innanzitutto, è necessario creare e abilitare una configurazione di controllo sulle macchine virtuali di storage (SVM). In secondo luogo, è necessario configurare i criteri di controllo nei file e nelle cartelle che si desidera monitorare. È possibile configurare criteri di controllo per monitorare i tentativi di accesso riusciti e non riusciti.

È possibile configurare policy di audit SMB e NFS. Le policy di audit SMB e NFS hanno requisiti di configurazione e funzionalità di audit differenti.

Se sono configurati i criteri di audit appropriati, ONTAP monitora gli eventi di accesso SMB e NFS come specificato nelle policy di audit solo se i server SMB o NFS sono in esecuzione.

Configurare le policy di audit su file e directory di sicurezza NTFS

Prima di poter controllare le operazioni di file e directory, è necessario configurare i criteri di audit sui file e sulle directory per cui si desidera raccogliere le informazioni di audit. Oltre all'impostazione e all'abilitazione della configurazione di audit. È possibile configurare i criteri di controllo NTFS utilizzando la scheda protezione di Windows o l'interfaccia utente di ONTAP.

Configurazione dei criteri di controllo NTFS mediante la scheda protezione di Windows

È possibile configurare i criteri di controllo NTFS su file e directory utilizzando la scheda **Windows Security** nella finestra Proprietà di Windows. Si tratta dello stesso metodo utilizzato per la configurazione dei criteri di controllo sui dati che risiedono su un client Windows, che consente di utilizzare la stessa interfaccia GUI utilizzata.

Di cosa hai bisogno

Il controllo deve essere configurato sulla macchina virtuale di storage (SVM) che contiene i dati a cui si

applicano gli elenchi di controllo di accesso al sistema (SACL).

A proposito di questa attività

La configurazione dei criteri di audit NTFS viene eseguita aggiungendo voci ai SACL NTFS associate a un descrittore di protezione NTFS. Il descrittore di protezione viene quindi applicato ai file e alle directory NTFS. Queste attività vengono gestite automaticamente dalla GUI di Windows. Il descrittore di protezione può contenere elenchi di controllo degli accessi discrezionali (DACL) per l'applicazione delle autorizzazioni di accesso a file e cartelle, SACL per il controllo di file e cartelle o SACL e DACL.

Per impostare i criteri di controllo NTFS utilizzando la scheda protezione di Windows, completare la seguente procedura su un host Windows:

Fasi

1. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
2. Completare la casella **Map Network Drive** (Connetti unità di rete):

   a. Selezionare una lettera **Drive**.

   b. Nella casella **Folder** (cartella), digitare il nome del server SMB che contiene la condivisione, contenente i dati che si desidera controllare e il nome della condivisione.

      È possibile specificare l'indirizzo IP dell'interfaccia dati per il server SMB invece del nome del server SMB.

      Se il nome del server SMB è "SMB_SERVER" e la condivisione è denominata "share1", immettere `\\SMB_SERVER\share1`.

   c. Fare clic su **fine**.

   Il disco selezionato viene montato e pronto con la finestra Esplora risorse che visualizza i file e le cartelle contenuti nella condivisione.

3. Selezionare il file o la directory per cui si desidera abilitare l'accesso di controllo.
4. Fare clic con il pulsante destro del mouse sul file o sulla directory, quindi selezionare **Proprietà**.
5. Selezionare la scheda **sicurezza**.
6. Fare clic su **Avanzate**.
7. Selezionare la scheda **Auditing**.
8. Eseguire le azioni desiderate:

Se si desidera	Effettuare le seguenti operazioni
Impostare il controllo per un nuovo utente o gruppo	a. Fare clic su **Aggiungi**. b. Nella casella immettere il nome dell'oggetto da selezionare, digitare il nome dell'utente o del gruppo che si desidera aggiungere. c. Fare clic su **OK**.

Rimuovere il controllo da un utente o gruppo	a. Nella casella immettere il nome dell'oggetto da selezionare, selezionare l'utente o il gruppo che si desidera rimuovere. b. Fare clic su **Rimuovi**. c. Fare clic su **OK**. d. Ignorare il resto di questa procedura.
Controllo delle modifiche per un utente o un gruppo	a. Nella casella immettere il nome dell'oggetto da selezionare, selezionare l'utente o il gruppo che si desidera modificare. b. Fare clic su **Edit** (Modifica). c. Fare clic su **OK**.

Se si imposta il controllo su un utente o un gruppo o si modifica il controllo su un utente o un gruppo esistente, viene visualizzata la casella voce di controllo per <object>.

9. Nella casella **Applica a**, selezionare la modalità di applicazione della voce di controllo.

   È possibile selezionare una delle seguenti opzioni:

   - **Questa cartella, sottocartelle e file**
   - **Questa cartella e sottocartelle**
   - **Solo questa cartella**
   - **Questa cartella e file**
   - **Solo sottocartelle e file**
   - **Solo sottocartelle**
   - **Solo file** se si imposta il controllo su un singolo file, la casella **Applica a** non è attiva. L'impostazione predefinita della casella **Applica a** è **solo questo oggetto**.

   > Poiché il controllo richiede risorse SVM, selezionare solo il livello minimo che fornisce gli eventi di controllo che soddisfano i requisiti di sicurezza.

10. Nella casella **Access**, selezionare i dati da sottoporre a verifica e se si desidera controllare gli eventi di successo, gli eventi di errore o entrambi.

    - Per controllare gli eventi riusciti, selezionare la casella Success (successo).
    - Per controllare gli eventi di errore, selezionare la casella Failure (errore).

      Selezionare solo le azioni da monitorare per soddisfare i requisiti di sicurezza. Per ulteriori informazioni su questi eventi verificabili, consultare la documentazione di Windows. È possibile controllare i seguenti eventi:

    - **Controllo completo**
    - **Cartella Traverse / file di esecuzione**
    - **Elenca cartella / leggi dati**
    - **Attributi di lettura**
    - **Leggi attributi estesi**

- **Creare file / scrivere dati**
- **Crea cartelle/Aggiungi dati**
- **Attributi di scrittura**
- **Scrivi attributi estesi**
- **Elimina sottocartelle e file**
- **Elimina**
- **Permessi di lettura**
- **Modifica delle autorizzazioni**
- **Assumere la proprietà**

11. Se non si desidera che l'impostazione di controllo si propaghi ai file e alle cartelle successivi del contenitore originale, selezionare la casella **Applica queste voci di controllo solo agli oggetti e/o ai contenitori all'interno di questo contenitore**.
12. Fare clic su **Apply** (Applica).
13. Dopo aver aggiunto, rimosso o modificato le voci di controllo, fare clic su **OK**.

    La casella voce di controllo per <object> viene chiusa.

14. Nella casella **Auditing**, selezionare le impostazioni di ereditarietà per questa cartella.

    Selezionare solo il livello minimo che fornisce gli eventi di controllo che soddisfano i requisiti di sicurezza. È possibile scegliere una delle seguenti opzioni:

    - Selezionare la casella Includi voci di controllo ereditabili dall'oggetto principale.
    - Selezionare la casella Sostituisci tutte le voci di controllo ereditabili esistenti su tutti i discendenti con voci di controllo ereditabili da questo oggetto.
    - Selezionare entrambe le caselle.
    - Selezionare nessuna delle due caselle. Se si impostano SACL su un singolo file, la casella di controllo Sostituisci tutte le voci di controllo ereditabili esistenti su tutti i discendenti con voci di controllo ereditabili da questo oggetto non è presente nella casella di controllo.

15. Fare clic su **OK**.

    La finestra Auditing si chiude.

Configurare i criteri di audit NTFS utilizzando l'interfaccia CLI di ONTAP

È possibile configurare i criteri di controllo su file e cartelle utilizzando l'interfaccia utente di ONTAP. Ciò consente di configurare le policy di audit NTFS senza la necessità di connettersi ai dati utilizzando una condivisione SMB su un client Windows.

È possibile configurare i criteri di audit NTFS utilizzando `vserver security file-directory` famiglia di comandi.

È possibile configurare SACL NTFS solo utilizzando la CLI. La configurazione dei SACL NFSv4 non è supportata con questa famiglia di comandi ONTAP. Consultare le pagine man per ulteriori informazioni sull'utilizzo di questi comandi per configurare e aggiungere SACL NTFS a file e cartelle.

Configurare il controllo per i file e le directory di sicurezza UNIX

È possibile configurare il controllo per i file e le directory di sicurezza UNIX aggiungendo ACE di controllo agli ACL NFSv4.x. Ciò consente di monitorare determinati eventi di accesso a file e directory NFS per motivi di sicurezza.

A proposito di questa attività

Per NFSv4.x, le ACE discrezionali e di sistema sono memorizzate nello stesso ACL. Non sono memorizzati in DACL e SACL separati. Pertanto, è necessario prestare attenzione quando si aggiungono ACE di audit a un ACL esistente per evitare di sovrascrivere e perdere un ACL esistente. L'ordine in cui si aggiungono le ACE di audit a un ACL esistente non ha importanza.

Fasi

1. Recuperare l'ACL esistente per il file o la directory utilizzando `nfs4_getfacl` o comando equivalente.

   Per ulteriori informazioni sulla manipolazione degli ACL, consulta le pagine man del tuo client NFS.

2. Aggiungere gli ACE di audit desiderati.
3. Applicare l'ACL aggiornato al file o alla directory utilizzando `nfs4_setfacl` o comando equivalente.

Visualizza informazioni sui criteri di controllo applicati a file e directory

Visualizzare le informazioni sui criteri di controllo utilizzando la scheda protezione di Windows

È possibile visualizzare informazioni sui criteri di controllo applicati a file e directory utilizzando la scheda Security (protezione) della finestra Windows Properties (Proprietà di Windows). Si tratta dello stesso metodo utilizzato per i dati residenti su un server Windows, che consente ai clienti di utilizzare la stessa interfaccia GUI a cui sono abituati.

A proposito di questa attività

La visualizzazione delle informazioni sui criteri di controllo applicati a file e directory consente di verificare che siano impostati gli elenchi di controllo di accesso di sistema (SACL) appropriati su file e cartelle specificati.

Per visualizzare informazioni sui SACL applicati a file e cartelle NTFS, completare la seguente procedura su un host Windows.

Fasi

1. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
2. Completare la finestra di dialogo **Map Network Drive** (Connetti unità di rete):

   a. Selezionare una lettera **Drive**.

   b. Nella casella **Folder** (cartella), digitare l'indirizzo IP o il nome del server SMB della macchina virtuale di storage (SVM) contenente la condivisione che contiene sia i dati che si desidera controllare che il nome della condivisione.

      Se il nome del server SMB è "SMB_SERVER" e la condivisione è denominata "share1", immettere `\\SMB_SERVER\share1`.

      > È possibile specificare l'indirizzo IP dell'interfaccia dati per il server SMB invece del nome del server SMB.

c. Fare clic su **fine**.

Il disco selezionato viene montato e pronto con la finestra Esplora risorse che visualizza i file e le cartelle contenuti nella condivisione.

3. Selezionare il file o la directory per cui vengono visualizzate le informazioni di controllo.
4. Fare clic con il pulsante destro del mouse sul file o sulla directory e selezionare **Proprietà**.
5. Selezionare la scheda **sicurezza**.
6. Fare clic su **Avanzate**.
7. Selezionare la scheda **Auditing**.
8. Fare clic su **continua**.

   Viene visualizzata la finestra Auditing. Nella casella **voci di controllo** viene visualizzato un riepilogo degli utenti e dei gruppi a cui sono stati applicati SACL.

9. Nella casella **voci di controllo** selezionare l'utente o il gruppo di cui si desidera visualizzare le voci SACL.
10. Fare clic su **Edit** (Modifica).

    Viene visualizzata la finestra voce di controllo per <object>.

11. Nella casella **Access**, visualizzare i SACL correnti applicati all'oggetto selezionato.
12. Fare clic su **Annulla** per chiudere la casella **voce di controllo per <object>**.
13. Fare clic su **Annulla** per chiudere la casella **controllo**.

Visualizza informazioni sui criteri di audit NTFS sui volumi FlexVol utilizzando l'interfaccia CLI

È possibile visualizzare informazioni sui criteri di controllo NTFS sui volumi FlexVol, inclusi gli stili di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sugli elenchi di controllo degli accessi al sistema. È possibile utilizzare le informazioni per convalidare la configurazione della protezione o per risolvere i problemi di controllo.

A proposito di questa attività

La visualizzazione delle informazioni sui criteri di controllo applicati a file e directory consente di verificare che siano impostati gli elenchi di controllo di accesso di sistema (SACL) appropriati su file e cartelle specificati.

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei file o delle cartelle di cui si desidera visualizzare le informazioni di audit. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree di sicurezza NTFS utilizzano solo SACL (System Access Control List) NTFS per i criteri di controllo.
- I file e le cartelle in un volume misto di sicurezza con protezione efficace NTFS possono applicare criteri di controllo NTFS.

  I volumi misti di sicurezza e le qtree possono contenere alcuni file e directory che utilizzano permessi di file UNIX, i bit di modalità o gli ACL NFSv4 e alcuni file e directory che utilizzano permessi di file NTFS.

- Il livello superiore di un volume misto di sicurezza può avere una protezione efficace UNIX o NTFS e potrebbe contenere o meno SACL NTFS.

- Poiché la protezione di Storage-Level Access Guard può essere configurata su un volume misto di sicurezza o qtree anche se lo stile di sicurezza effettivo della root del volume o del qtree è UNIX, L'output di un volume o percorso qtree in cui Storage-Level Access Guard è configurato potrebbe visualizzare sia SACL NFSv4 di file e cartelle standard che SACL NTFS di Storage-Level Access Guard.
- Se il percorso immesso nel comando è relativo ai dati con protezione effettiva NTFS, l'output visualizza anche le informazioni relative alle ACE di controllo dinamico degli accessi se Dynamic Access Control è configurato per il percorso di file o directory specificato.
- Quando si visualizzano informazioni di sicurezza su file e cartelle con protezione efficace NTFS, i campi di output relativi a UNIX contengono informazioni di autorizzazione file UNIX di sola visualizzazione.

  I file e le cartelle di sicurezza NTFS utilizzano solo le autorizzazioni per i file NTFS e gli utenti e i gruppi Windows per determinare i diritti di accesso ai file.

- L'output ACL viene visualizzato solo per file e cartelle con protezione NTFS o NFSv4.

  Questo campo è vuoto per i file e le cartelle che utilizzano la protezione UNIX e che dispongono solo delle autorizzazioni di bit di modalità applicate (nessun ACL NFSv4).

- I campi owner e group output nell'output ACL sono validi solo nel caso di descrittori di protezione NTFS.

Fase

1. Visualizzare le impostazioni dei criteri di controllo di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni…	Immettere il seguente comando…
In forma riassuntiva	`vserver security file-directory show -vserver vserver_name -path path`
Come elenco dettagliato	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative ai criteri di controllo per il percorso `/corp` In SVM vs1. Il percorso offre una protezione efficace con NTFS. Il descrittore di protezione NTFS contiene sia una voce SACL RIUSCITA che UNA SACL RIUSCITA/NON RIUSCITA.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative ai criteri di controllo per il percorso `/datavol1` In SVM vs1. Il percorso contiene SACL di file e cartelle e SACL Storage-Level Access Guard.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Modi per visualizzare informazioni sulla sicurezza dei file e sulle policy di audit

È possibile utilizzare il carattere jolly (*) per visualizzare informazioni sulla sicurezza dei file e sulle policy di controllo di tutti i file e le directory in un determinato percorso o

volume root.

Il carattere jolly (*) può essere utilizzato come ultimo sottocomponente di un determinato percorso di directory al di sotto del quale si desidera visualizzare le informazioni di tutti i file e le directory.

Se si desidera visualizzare le informazioni di un determinato file o directory denominata "*", è necessario fornire il percorso completo tra virgolette doppie (" ").

Esempio

Il seguente comando con il carattere jolly visualizza le informazioni su tutti i file e le directory sotto il percorso `/1/` Di SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

Il seguente comando visualizza le informazioni di un file denominato "*" sotto il percorso `/vol1/a` Di SVM vs1. Il percorso è racchiuso tra virgolette doppie (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                 Vserver: vs1
               File Path: “/vol1/a/*”
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

CLI modifica gli eventi che possono essere verificati

Panoramica degli eventi di cambiamento CLI che possono essere verificati

ONTAP è in grado di controllare alcuni eventi di modifica dell’interfaccia CLI, tra cui determinati eventi di condivisione SMB, determinati eventi dei criteri di controllo, determinati eventi dei gruppi di protezione locali, eventi dei gruppi di utenti locali ed eventi dei criteri di autorizzazione. La comprensione degli eventi di modifica che è possibile verificare è utile quando si interpretano i risultati dei registri degli eventi.

È possibile gestire la macchina virtuale dello storage (SVM) per il controllo degli eventi di modifica della CLI ruotando manualmente i registri di controllo, attivando o disattivando il controllo, visualizzando le informazioni relative al controllo degli eventi di modifica, modificando gli eventi di modifica del controllo ed eliminando gli eventi di modifica del controllo.

In qualità di amministratore, se si esegue un comando per modificare la configurazione relativa agli eventi SMB-share, User-group locale, Security-group locale, Authorization-policy e audit-policy, viene generato un record e viene verificato l’evento corrispondente:

Categoria di controllo	Eventi	ID evento	Eseguire questo comando…

Mhost Auditing	cambiamento di policy	[4719] Configurazione dell'audit modificata	`vserver audit disable
enable	modify`	condivisione file	[5142] è stata aggiunta la condivisione di rete
`vserver cifs share create`	[5143] la condivisione di rete è stata modificata	`vserver cifs share modify` `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] condivisione di rete eliminata	`vserver cifs share delete`
Controllo	account utente	[4720] utente locale creato	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722] utente locale abilitato	`vserver cifs users-and-groups local-user create	modify`	[4724] reimpostazione della password utente locale
`vserver cifs users-and-groups local-user set-password`	[4725] utente locale disattivato	`vserver cifs users-and-groups local-user create	modify`
[4726] utente locale cancellato	`vserver cifs users-and-groups local-user delete` `vserver services name-service unix-user delete`	[4738] Modifica utente locale	`vserver cifs users-and-groups local-user modify` `vserver services name-service unix-user modify`
[4781] Rinomina utente locale	`vserver cifs users-and-groups local-user rename`	security-group	[4731] Gruppo di sicurezza locale creato
`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`	[4734] Gruppo di sicurezza locale cancellato	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`	[4735] Gruppo di sicurezza locale modificato

`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732] utente aggiunto al gruppo locale	`vserver cifs users-and-groups local-group add-members` `vserver services name-service unix-group adduser`
[4733] utente rimosso dal gruppo locale	`vserver cifs users-and-groups local-group remove-members` `vserver services name-service unix-group deluser`	authorization-policy-change	[4704] diritti utente assegnati
`vserver cifs users-and-groups privilege add-privilege`	[4705] diritti utente rimossi	`vserver cifs users-and-groups privilege remove-privilege	reset-privilege`

Gestire l'evento di condivisione file

Quando viene configurato un evento di condivisione file per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit. Gli eventi di condivisione file vengono generati quando la condivisione di rete SMB viene modificata utilizzando `vserver cifs share` comandi correlati.

Gli eventi di file-share con gli id evento 5142, 5143 e 5144 vengono generati quando una condivisione di rete SMB viene aggiunta, modificata o eliminata per la SVM. La configurazione della condivisione di rete SMB viene modificata utilizzando `cifs share access control create|modify|delete` comandi.

Nell'esempio seguente viene visualizzato un evento di condivisione file con ID 5143, quando viene creato un oggetto di condivisione denominato 'audit_dest':

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

Gestire l'evento audit-policy-change

Quando viene configurato un evento audit-policy-change per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit. Gli eventi audit-policy-change vengono generati quando un criterio di audit viene modificato utilizzando `vserver audit` comandi correlati.

L'evento audit-policy-change con l'id evento 4719 viene generato ogni volta che un criterio di audit viene disattivato, attivato o modificato e aiuta a identificare quando un utente tenta di disattivare il controllo per coprire le tracce. È configurato per impostazione predefinita e richiede il privilegio di diagnostica per la disattivazione.

Nell'esempio riportato di seguito viene visualizzato un evento di modifica della policy di audit con l'ID 4719 generato, quando un audit viene disattivato:

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

Gestire l'evento dell'account utente

Quando viene configurato un evento account utente per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit.

Gli eventi dell'account utente con id evento 4720, 4722, 4724, 4725, 4726, 4738 e 4781 vengono generati quando un utente SMB o NFS locale viene creato o cancellato dal sistema, l'account utente locale viene attivato, disattivato o modificato e la password utente SMB locale viene reimpostata o modificata. Gli eventi dell'account utente vengono generati quando un account utente viene modificato utilizzando `vserver cifs users-and-groups <local user>` e. `vserver services name-service <unix user>` comandi.

Nell'esempio seguente viene visualizzato un evento dell'account utente con l'ID 4720 generato, quando viene creato un utente SMB locale:

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

Nell'esempio seguente viene visualizzato un evento dell'account utente con l'ID 4781 generato, quando l'utente SMB locale creato nell'esempio precedente viene rinominato:

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

Gestire gli eventi del gruppo di sicurezza

Quando viene configurato un evento di gruppo di sicurezza per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit.

Gli eventi del gruppo di sicurezza con id evento 4731, 4732, 4733, 4734 e 4735 vengono generati quando un gruppo SMB o NFS locale viene creato o cancellato dal sistema e l'utente locale viene aggiunto o rimosso dal gruppo. Gli eventi-gruppo-sicurezza vengono generati quando un account utente viene modificato utilizzando `vserver cifs users-and-groups <local-group>` e. `vserver services name-service <unix-group>` comandi.

Nell'esempio seguente viene visualizzato un evento del gruppo di protezione con l'ID 4731 generato quando viene creato un gruppo di protezione UNIX locale:

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

Gestire l'evento Authorization-policy-change

Quando l'evento Authorization-policy-change viene configurato per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit.

Gli eventi Authorization-policy-change con ID evento 4704 e 4705 vengono generati ogni volta che vengono concessi o revocati i diritti di autorizzazione per un utente SMB e un gruppo SMB. Gli eventi Authorization-policy-change vengono generati quando i diritti di autorizzazione vengono assegnati o revocati utilizzando `vserver cifs users-and-groups privilege` comandi correlati.

Nell'esempio seguente viene visualizzato un evento del criterio di autorizzazione con l'ID 4704 generato, quando vengono assegnati i diritti di autorizzazione per un gruppo di utenti SMB:

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

Gestire le configurazioni di controllo

Ruotare manualmente i registri degli eventi di audit

Prima di poter visualizzare i registri degli eventi di audit, è necessario convertirli in formati leggibili dall'utente. Se si desidera visualizzare i registri degli eventi per una specifica macchina virtuale di storage prima che ONTAP ruoti automaticamente il registro, è possibile ruotare manualmente i registri degli eventi di audit su una SVM.

Fase

1. Ruotare i registri degli eventi di audit utilizzando `vserver audit rotate-log` comando.

   ```
   vserver audit rotate-log -vserver vs1
   ```

   Il registro eventi di audit viene salvato nella directory del registro eventi di audit SVM con il formato specificato dalla configurazione di audit (`XML` oppure `EVTX`), e possono essere visualizzati utilizzando l'applicazione appropriata.

Abilitare e disabilitare il controllo sulle SVM

È possibile attivare o disattivare il controllo sulle macchine virtuali di storage (SVM). È possibile interrompere temporaneamente il controllo di file e directory disattivando il controllo. È possibile attivare il controllo in qualsiasi momento (se esiste una configurazione di controllo).

Di cosa hai bisogno

Prima di poter attivare il controllo su SVM, la configurazione di controllo di SVM deve già esistere.

"Creare la configurazione di controllo"

A proposito di questa attività

La disattivazione del controllo non elimina la configurazione del controllo.

Fasi

1. Eseguire il comando appropriato:

Se si desidera che il controllo sia…	Immettere il comando…
Attivato	`vserver audit enable -vserver vserver_name`
Disattivato	`vserver audit disable -vserver vserver_name`

2. Verificare che il controllo si trovi nello stato desiderato:

   ```
   vserver audit show -vserver vserver_name
   ```

Esempi

Nell'esempio seguente viene attivato il controllo per SVM vs1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                           Log Format: evtx
                  Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

Nell'esempio seguente viene disattivato il controllo per SVM vs1:

```
cluster1::> vserver audit disable -vserver vs1

                              Vserver: vs1
                      Auditing state: false
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                  Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                   Rotation Schedules: -
            Log Files Rotation Limit: 10
```

Visualizzare le informazioni relative al controllo delle configurazioni

È possibile visualizzare le informazioni relative al controllo delle configurazioni. Le informazioni consentono di determinare se la configurazione è quella desiderata per ogni SVM. Le informazioni visualizzate consentono inoltre di verificare se è attivata una configurazione di controllo.

A proposito di questa attività

È possibile visualizzare informazioni dettagliate sulle configurazioni di controllo su tutte le SVM oppure personalizzare le informazioni visualizzate nell'output specificando i parametri opzionali. Se non si specifica alcun parametro opzionale, viene visualizzato quanto segue:

- Nome SVM a cui si applica la configurazione di controllo
- Lo stato di audit, che può essere `true` oppure `false`

  Se lo stato di audit è `true`, il controllo è attivato. Se lo stato di audit è `false`, il controllo è disattivato.

- Le categorie di eventi da controllare
- Il formato del registro di controllo
- La directory di destinazione in cui il sottosistema di controllo memorizza i registri di controllo consolidati e convertiti

Fase

1. Visualizzare le informazioni sulla configurazione di controllo utilizzando `vserver audit show` comando.

   Per ulteriori informazioni sull'utilizzo del comando, vedere le pagine man.

Esempi

Nell'esempio seguente viene visualizzato un riepilogo della configurazione di controllo per tutte le SVM:

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

Nell'esempio seguente vengono visualizzate, sotto forma di elenco, tutte le informazioni di configurazione per il controllo di tutte le SVM:

```
cluster1::> vserver audit show -instance

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                           Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
```

Comandi per la modifica delle configurazioni di controllo

Se si desidera modificare un'impostazione di controllo, è possibile modificare la configurazione corrente in qualsiasi momento, tra cui la modifica della destinazione del percorso di log e del formato di log, la modifica delle categorie di eventi da controllare, la modalità di salvataggio automatico dei file di log e il numero massimo di file di log da salvare.

Se si desidera…	Utilizzare questo comando…
Modificare il percorso di destinazione del log	`vserver audit modify` con `-destination` parametro

Modificare la categoria di eventi da controllare	`vserver audit modify` con `-events` parametro Per controllare gli eventi di staging dei criteri di accesso centrale, è necessario attivare l'opzione del server SMB DAC (Dynamic Access Control) sulla macchina virtuale di storage (SVM).
Modificare il formato del registro	`vserver audit modify` con `-format` parametro
Attivazione dei salvataggi automatici in base alle dimensioni interne del file di log	`vserver audit modify` con `-rotate-size` parametro
Attivazione dei salvataggi automatici in base a un intervallo di tempo	`vserver audit modify` con `-rotate-schedule-month`, `-rotate-schedule-dayofweek`, `-rotate-schedule-day`, `-rotate-schedule-hour`, e. `-rotate-schedule-minute` parametri
Specifica del numero massimo di file di log salvati	`vserver audit modify` con `-rotate-limit` parametro

Eliminare una configurazione di controllo

Se non si desidera più controllare gli eventi di file e directory sulla macchina virtuale di storage (SVM) e non si desidera mantenere una configurazione di controllo sulla SVM, è possibile eliminare la configurazione di controllo.

Fasi

1. Disattivare la configurazione di controllo:

   ```
   vserver audit disable -vserver vserver_name
   ```

   ```
   vserver audit disable -vserver vs1
   ```

2. Eliminare la configurazione di controllo:

   ```
   vserver audit delete -vserver vserver_name
   ```

   ```
   vserver audit delete -vserver vs1
   ```

Comprendere le implicazioni del ripristino del cluster

Se si prevede di ripristinare il cluster, è necessario conoscere il processo di revert che ONTAP segue quando nel cluster sono presenti macchine virtuali di storage abilitate per l'auditing. È necessario eseguire determinate azioni prima di eseguire il ripristino.

Ripristino di una versione di ONTAP che non supporta il controllo degli eventi di logon e logoff SMB e degli eventi di staging dei criteri di accesso centrale

Il supporto per il controllo degli eventi di logon e logoff SMB e per gli eventi di staging dei criteri di accesso centrale inizia con Clustered Data ONTAP 8.3. Se si ripristina una versione di ONTAP che non supporta questi tipi di eventi e si dispone di configurazioni di controllo che monitorano questi tipi di eventi, è necessario modificare la configurazione di controllo per tali SVM abilitate all'audit prima di eseguire il ripristino. È necessario modificare la configurazione in modo che vengano controllati solo gli eventi del file-op.

Risolvere i problemi di auditing e di gestione dello spazio dei volumi

Possono verificarsi problemi quando lo spazio disponibile sui volumi di staging o sul volume contenente i registri degli eventi di audit è insufficiente. Se lo spazio è insufficiente, non è possibile creare nuovi record di audit, impedendo ai client di accedere ai dati e impedendo l'esecuzione delle richieste di accesso. Dovresti sapere come risolvere questi problemi di spazio del volume.

Risolvere i problemi di spazio relativi ai volumi del registro eventi

Se i volumi contenenti file di log degli eventi esauriranno lo spazio, il controllo non potrà convertire i record di log in file di log. Ciò comporta errori di accesso al client. È necessario sapere come risolvere i problemi di spazio relativi ai volumi del registro eventi.

- Gli amministratori delle macchine virtuali di storage (SVM) e dei cluster possono determinare se lo spazio dei volumi è insufficiente visualizzando informazioni sull'utilizzo e la configurazione dei volumi e degli aggregati.
- Se lo spazio disponibile nei volumi contenenti registri eventi è insufficiente, gli amministratori di SVM e cluster possono risolvere i problemi di spazio rimuovendo alcuni file di registro eventi o aumentando le dimensioni del volume.

> Se l'aggregato che contiene il volume del registro eventi è pieno, è necessario aumentare le dimensioni dell'aggregato prima di poter aumentare le dimensioni del volume. Solo un amministratore del cluster può aumentare le dimensioni di un aggregato.

- Il percorso di destinazione dei file di registro eventi può essere modificato in una directory di un altro volume modificando la configurazione di controllo.

> L'accesso ai dati viene negato nei seguenti casi:
>
> - Se la directory di destinazione viene eliminata.
> - Se il limite di file su un volume, che ospita la directory di destinazione, raggiunge il livello massimo.

Scopri di più su:

- "Come visualizzare informazioni sui volumi e aumentare le dimensioni del volume".
- "Come visualizzare informazioni sugli aggregati e sulla gestione degli aggregati".

Risolvere i problemi di spazio relativi ai volumi di staging

Se uno dei volumi contenenti file di staging per la macchina virtuale di storage (SVM) esaurisce lo spazio, il controllo non può scrivere record di log nei file di staging. Ciò comporta errori di accesso al client. Per risolvere questo problema, è necessario determinare se uno dei volumi di staging utilizzati nella SVM è pieno visualizzando le informazioni sull'utilizzo del volume.

Se il volume contenente i file di registro eventi consolidati dispone di spazio sufficiente ma si verificano ancora errori di accesso del client a causa di spazio insufficiente, i volumi di staging potrebbero essere fuori spazio. L'amministratore di SVM deve contattare l'utente per determinare se i volumi di staging che contengono file di staging per SVM hanno spazio insufficiente. Il sottosistema di controllo genera un evento EMS se non è possibile generare eventi di controllo a causa dello spazio insufficiente in un volume di staging. Viene visualizzato il seguente messaggio: `No space left on device`. Solo gli amministratori SVM possono visualizzare informazioni sui volumi di staging.

Tutti i nomi dei volumi di staging iniziano con `MDV_aud_` Seguito dall'UUID dell'aggregato contenente il volume di staging. L'esempio seguente mostra quattro volumi di sistema sulla SVM amministrativa, creati automaticamente quando è stata creata una configurazione di controllo dei file service per una SVM di dati nel cluster:

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          2GB     1.90GB
5%
4 entries were displayed.
```

Se lo spazio disponibile nei volumi di staging è insufficiente, è possibile risolvere i problemi di spazio aumentando le dimensioni del volume.

> Se l'aggregato che contiene il volume di staging è pieno, è necessario aumentare le dimensioni dell'aggregato prima di poter aumentare le dimensioni del volume. Solo gli amministratori di SVM possono aumentare le dimensioni di un aggregato.

Se uno o più aggregati hanno uno spazio disponibile inferiore a 2 GB, la creazione dell'audit SVM non riesce. Quando la creazione dell'audit SVM non riesce, i volumi di staging creati vengono cancellati.

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

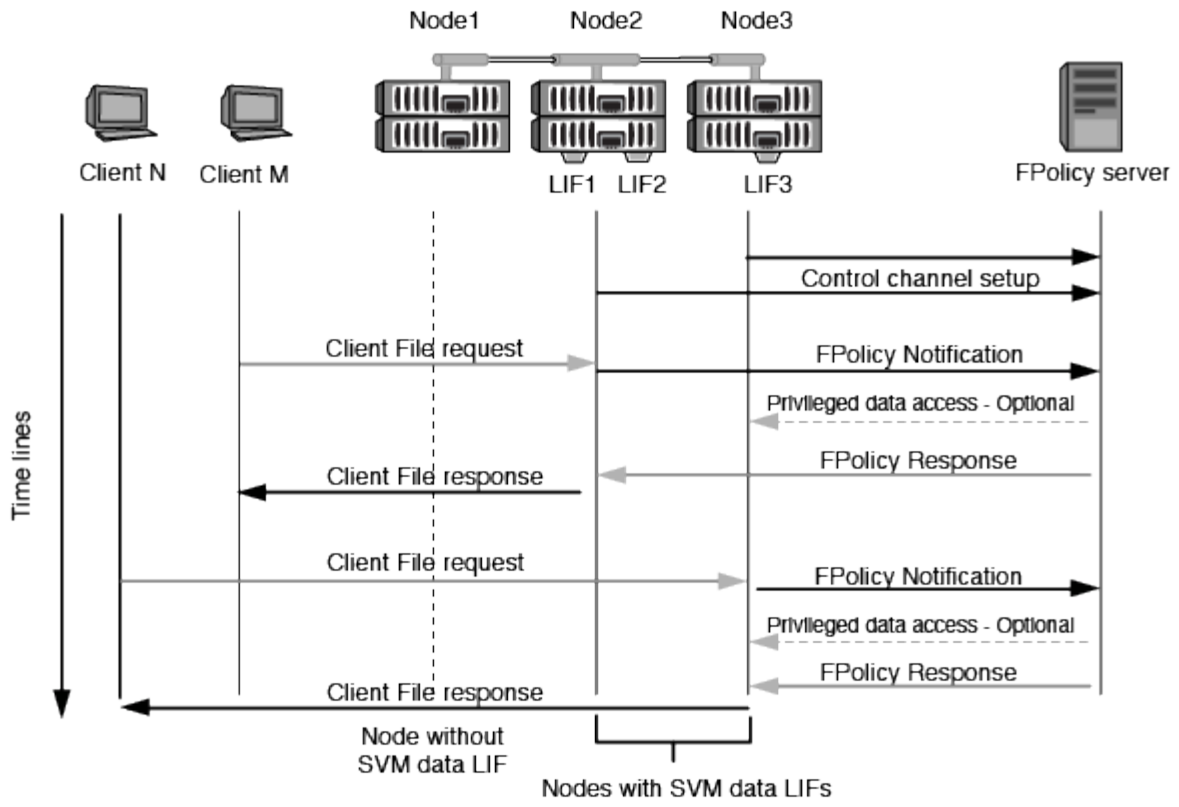
Per pianificare correttamente la configurazione di FPolicy, è necessario comprendere il processo di comunicazione da nodo a server FPolicy esterno.

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
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

Contatori	Descrizione
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.

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
```

Verificare l’accesso utilizzando il tracciamento di sicurezza

Come funzionano le tracce di sicurezza

È possibile aggiungere filtri di tracciamento delle autorizzazioni per indicare a ONTAP di registrare le informazioni sul motivo per cui i server SMB e NFS su una macchina virtuale di storage (SVM) consentono o negano la richiesta di un client o di un utente di eseguire un’operazione. Ciò può essere utile quando si desidera verificare che lo schema di protezione per l’accesso ai file sia appropriato o quando si desidera risolvere i problemi di accesso ai file.

Le tracce di sicurezza consentono di configurare un filtro che rileva le operazioni client su SMB e NFS su SVM e di tracciare tutti i controlli di accesso corrispondenti a tale filtro. È quindi possibile visualizzare i risultati della traccia, che fornisce un pratico riepilogo del motivo per cui l’accesso è stato consentito o negato.

Se si desidera verificare le impostazioni di sicurezza per l’accesso SMB o NFS su file e cartelle su SVM o se si verifica un problema di accesso, è possibile aggiungere rapidamente un filtro per attivare il tracciamento delle autorizzazioni.

Il seguente elenco illustra importanti informazioni sul funzionamento delle tracce di protezione:

- ONTAP applica le tracce di sicurezza a livello di SVM.
- Ogni richiesta in entrata viene sottoposta a screening per verificare se corrisponde ai criteri di filtraggio di eventuali tracce di sicurezza attivate.
- Le tracce vengono eseguite per le richieste di accesso a file e cartelle.
- Le tracce possono filtrare in base ai seguenti criteri:
  - IP client
  - Percorso SMB o NFS
  - Nome di Windows
  - Nome UNIX

- Le richieste vengono sottoposte a screening per i risultati delle risposte di accesso *consentito* e *negato*.
- Ogni richiesta di criteri di filtraggio corrispondenti delle tracce attivate viene registrata nel log dei risultati della traccia.
- L'amministratore dello storage può configurare un timeout su un filtro per disattivarlo automaticamente.
- Se una richiesta corrisponde a più filtri, vengono registrati i risultati del filtro con il numero di indice più alto.
- L'amministratore dello storage può stampare i risultati dal log dei risultati della traccia per determinare il motivo per cui una richiesta di accesso è stata consentita o negata.

Tipi di controllo degli accessi monitorano le tracce di sicurezza

I controlli di accesso per un file o una cartella vengono eseguiti in base a criteri multipli. Le tracce di sicurezza monitorano le operazioni su tutti questi criteri.

I tipi di controlli degli accessi monitorati dalle tracce di protezione includono quanto segue:

- Stile di sicurezza del volume e del qtree
- Sicurezza effettiva del file system contenente i file e le cartelle su cui sono richieste le operazioni
- Mappatura dell'utente
- Permessi a livello di condivisione
- Permessi a livello di esportazione
- Permessi a livello di file
- Sicurezza di Access Guard a livello di storage

Considerazioni per la creazione di tracce di protezione

Quando si creano tracce di sicurezza sulle macchine virtuali di storage (SVM), è necessario tenere a mente diverse considerazioni. Ad esempio, è necessario conoscere i protocolli che è possibile creare una traccia, gli stili di protezione supportati e il numero massimo di tracce attive.

- È possibile creare tracce di sicurezza solo sulle SVM.
- Ogni voce di filtro di traccia di protezione è specifica per SVM.

  Specificare la SVM su cui si desidera eseguire la traccia.

- È possibile aggiungere filtri di tracciamento delle autorizzazioni per le richieste SMB e NFS.
- È necessario configurare il server SMB o NFS sulla SVM su cui si desidera creare i filtri di traccia.
- È possibile creare tracce di sicurezza per file e cartelle che risiedono su NTFS, UNIX e volumi e qtree misti di sicurezza.
- È possibile aggiungere un massimo di 10 filtri di tracciamento delle autorizzazioni per SVM.
- Quando si crea o si modifica un filtro, è necessario specificare un numero di indice del filtro.

  I filtri vengono considerati in ordine del numero di indice. I criteri di un filtro con un numero di indice superiore vengono considerati prima dei criteri con un numero di indice inferiore. Se la richiesta tracciata corrisponde ai criteri in più filtri abilitati, viene attivato solo il filtro con il numero di indice più alto.

- Dopo aver creato e attivato un filtro di traccia di protezione, è necessario eseguire alcune richieste di file o cartelle su un sistema client per generare attività che il filtro di traccia può acquisire e accedere al registro dei risultati di traccia.
- È necessario aggiungere filtri di tracciamento delle autorizzazioni solo per la verifica dell'accesso al file o per la risoluzione dei problemi.

  L'aggiunta di filtri di tracciamento delle autorizzazioni ha un effetto minore sulle prestazioni del controller.

  Una volta completata l'attività di verifica o risoluzione dei problemi, è necessario disattivare o rimuovere tutti i filtri di tracciamento delle autorizzazioni. Inoltre, i criteri di filtraggio selezionati devono essere il più specifici possibile, in modo che ONTAP non invii un numero elevato di risultati di traccia al registro.

Eseguire le tracce di sicurezza

Eseguire una panoramica delle tracce di sicurezza

L'esecuzione di una traccia di protezione implica la creazione di un filtro di traccia di protezione, la verifica dei criteri di filtro, la generazione di richieste di accesso su un client SMB o NFS che corrispondono ai criteri di filtro e la visualizzazione dei risultati.

Dopo aver utilizzato un filtro di sicurezza per acquisire le informazioni di traccia, è possibile modificare il filtro e riutilizzarlo oppure disattivarlo se non è più necessario. Dopo aver visualizzato e analizzato i risultati della traccia del filtro, è possibile eliminarli se non sono più necessari.

Creare filtri di traccia per la sicurezza

È possibile creare filtri di traccia per la sicurezza che rilevano le operazioni dei client SMB e NFS sulle macchine virtuali di storage (SVM) e tracciano tutti i controlli di accesso corrispondenti al filtro. È possibile utilizzare i risultati delle tracce di protezione per convalidare la configurazione o risolvere i problemi di accesso.

A proposito di questa attività

Sono necessari due parametri per il comando vserver Security trace filter create:

Parametri richiesti	Descrizione
`-vserver vserver_name`	*Nome SVM* Il nome della SVM che contiene i file o le cartelle su cui si desidera applicare il filtro di traccia di protezione.
`-index index_number`	*Numero indice del filtro* Il numero di indice che si desidera applicare al filtro. È possibile utilizzare un massimo di 10 filtri di traccia per SVM. I valori consentiti per questo parametro sono compresi tra 1 e 10.

Una serie di parametri di filtro opzionali consente di personalizzare il filtro di traccia di protezione in modo da restringere i risultati prodotti dalla traccia di protezione:

Parametro del filtro	Descrizione
`-client-ip IP_Address`	Questo filtro specifica l'indirizzo IP da cui l'utente accede a SVM.
`-path path`	Questo filtro specifica il percorso su cui applicare il filtro di traccia delle autorizzazioni. Il valore per `-path` può utilizzare uno dei seguenti formati: • Il percorso completo, a partire dalla directory principale della condivisione o dell'esportazione • Un percorso parziale, relativo alla radice della condivisione È necessario utilizzare i separatori di directory in stile UNIX di NFS nel valore del percorso.
`-windows-name win_user_name` oppure `-unix -name``unix_user_name`	È possibile specificare il nome utente Windows o UNIX di cui si desidera tenere traccia delle richieste di accesso. La variabile del nome utente non fa distinzione tra maiuscole e minuscole. Non è possibile specificare un nome utente Windows e un nome utente UNIX nello stesso filtro. Anche se è possibile tracciare gli eventi di accesso SMB e NFS, l'utente UNIX mappato e i gruppi di utenti UNIX mappati potrebbero essere utilizzati quando si eseguono controlli di accesso su dati misti o UNIX di tipo di sicurezza.
`-trace-allow` {`yes`	`no`}
La funzione di traccia per gli eventi di negazione è sempre abilitata per un filtro di traccia di protezione. Facoltativamente, è possibile tracciare gli eventi Allow. Per tracciare gli eventi Allow, impostare questo parametro su `yes`.	`-enabled` {`enabled`
`disabled`}	È possibile attivare o disattivare il filtro di traccia di protezione. Per impostazione predefinita, il filtro di traccia di protezione è attivato.
`-time-enabled integer`	È possibile specificare un timeout per il filtro, dopo il quale viene disattivato.

Fasi

1. Creazione di un filtro di traccia per la protezione:

   ```
   vserver security trace filter create -vserver vserver_name -index
   index_numberfilter_parameters
   ```

`filter_parameters` è un elenco di parametri di filtro opzionali.

Per ulteriori informazioni, vedere le pagine man del comando.

2. Verificare la voce Security trace filter:

```
vserver security trace filter show -vserver vserver_name -index index_number
```

Esempi

Il comando seguente crea un filtro di traccia di protezione per qualsiasi utente che accede a un file con un percorso di condivisione `\\server\share1\dir1\dir2\file.txt` Dall'indirizzo IP 10.10.10.7. Il filtro utilizza un percorso completo per `-path` opzione. L'indirizzo IP del client utilizzato per accedere ai dati è 10.10.10.7. Il filtro si esaurisce dopo 30 minuti:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
```

Il comando seguente crea un filtro di traccia di protezione utilizzando un percorso relativo per `-path` opzione. Il filtro traccia l'accesso di un utente Windows chiamato "joe". Joe sta accedendo a un file con un percorso di condivisione `\\server\share1\dir1\dir2\file.txt`. Le tracce del filtro consentono e negano gli eventi:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                                Vserver: vs1
                           Filter Index: 2
              Client IP Address to Match: -
                                   Path: /dir1/dir2/file.txt
                     Windows User Name: mydomain\joe
                        UNIX User Name: -
                    Trace Allow Events: yes
                        Filter Enabled: enabled
                Minutes Filter is Enabled: 60
```

Visualizza informazioni sui filtri di traccia per la sicurezza

È possibile visualizzare informazioni sui filtri di traccia di protezione configurati sulla macchina virtuale di storage (SVM). In questo modo è possibile visualizzare i tipi di eventi di accesso che ciascun filtro traccia.

Fase

1. Visualizzare le informazioni relative alle voci del filtro di traccia di protezione utilizzando `vserver security trace filter show` comando.

   Per ulteriori informazioni sull'utilizzo di questo comando, vedere le pagine man.

Esempi

Il seguente comando visualizza informazioni su tutti i filtri di traccia di sicurezza su SVM vs1:

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

Visualizzare i risultati della traccia di sicurezza

È possibile visualizzare i risultati della traccia di protezione generati per le operazioni dei file che corrispondono ai filtri di traccia di protezione. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza per l'accesso ai file o per risolvere i problemi di accesso ai file SMB e NFS.

Di cosa hai bisogno

Per generare i risultati della traccia di protezione, è necessario che esista un filtro di traccia di protezione abilitato e che siano state eseguite operazioni da un client SMB o NFS che corrisponda al filtro di traccia di protezione.

A proposito di questa attività

È possibile visualizzare un riepilogo di tutti i risultati della traccia di protezione oppure personalizzare le informazioni visualizzate nell'output specificando parametri opzionali. Ciò può essere utile quando i risultati della traccia di protezione contengono un gran numero di record.

Se non si specifica alcun parametro opzionale, viene visualizzato quanto segue:

- Nome SVM (Storage Virtual Machine)
- Nome del nodo
- Numero di indice della traccia di sicurezza
- Stile di sicurezza
- Percorso
- Motivo
- Nome utente

  Il nome utente viene visualizzato in base alla configurazione del filtro di traccia:

Se il filtro è configurato…	Quindi…
Con un nome utente UNIX	Il risultato della traccia di protezione visualizza il nome utente UNIX.
Con un nome utente Windows	Il risultato della traccia di protezione visualizza il nome utente di Windows.
Senza nome utente	Il risultato della traccia di protezione visualizza il nome utente di Windows.

È possibile personalizzare l'output utilizzando parametri opzionali. Alcuni dei parametri facoltativi che è possibile utilizzare per limitare i risultati restituiti nell'output del comando includono:

Parametro facoltativo	Descrizione
`-fields field_name, ...`	Visualizza l'output nei campi scelti. È possibile utilizzare questo parametro da solo o in combinazione con altri parametri opzionali.
`-instance`	Visualizza informazioni dettagliate sugli eventi di analisi della sicurezza. Utilizzare questo parametro con altri parametri opzionali per visualizzare informazioni dettagliate sui risultati specifici del filtro.
`-node node_name`	Visualizza solo informazioni sugli eventi nel nodo specificato.
`-vserver vserver_name`	Visualizza solo le informazioni sugli eventi sulla SVM specificata.
`-index integer`	Visualizza le informazioni sugli eventi che si sono verificati come risultato del filtro corrispondente al numero di indice specificato.
`-client-ip IP_address`	Visualizza informazioni sugli eventi che si sono verificati in seguito all'accesso al file dall'indirizzo IP del client specificato.
`-path path`	Visualizza le informazioni sugli eventi che si sono verificati in seguito all'accesso al file al percorso specificato.
`-user-name user_name`	Visualizza informazioni sugli eventi che si sono verificati in seguito all'accesso al file da parte dell'utente Windows o UNIX specificato.
`-security-style security_style`	Visualizza informazioni sugli eventi che si sono verificati nei file system con lo stile di sicurezza specificato.

Consultare la pagina man per informazioni sugli altri parametri opzionali che è possibile utilizzare con il comando.

Fase

1. Visualizzare i risultati del filtro di traccia di protezione utilizzando `vserver security trace trace-`

`result show` comando.

```
vserver security trace trace-result show -user-name domain\user
```

```
Vserver: vs1

Node     Index   Filter Details         Reason
-------- ------- ---------------------  ----------------------------
node1    3       User:domain\user       Access denied by explicit ACE
                 Security Style:mixed
                 Path:/dir1/dir2/

node1    5       User:domain\user       Access denied by explicit ACE
                 Security Style:unix
                 Path:/dir1/
```

Modificare i filtri di traccia di protezione

Se si desidera modificare i parametri di filtro opzionali utilizzati per determinare gli eventi di accesso da tracciare, è possibile modificare i filtri di traccia di protezione esistenti.

A proposito di questa attività

È necessario identificare il filtro di traccia di protezione che si desidera modificare specificando il nome della macchina virtuale di storage (SVM) a cui è applicato il filtro e il numero di indice del filtro. È possibile modificare tutti i parametri del filtro opzionali.

Fasi

1. Modificare un filtro di traccia di protezione:

   ```
   vserver security trace filter modify -vserver vserver_name -index
   index_numberfilter_parameters
   ```

   - `vserver_name` È il nome della SVM su cui si desidera applicare un filtro di traccia di protezione.
   - `index_number` è il numero di indice che si desidera applicare al filtro. I valori consentiti per questo parametro sono compresi tra 1 e 10.
   - `filter_parameters` è un elenco di parametri di filtro opzionali.
2. Verificare la voce Security trace filter:

   ```
   vserver security trace filter show -vserver vserver_name -index index_number
   ```

Esempio

Il comando seguente modifica il filtro di traccia di protezione con il numero di indice 1. Il filtro traccia gli eventi di qualsiasi utente che accede a un file con un percorso di condivisione `\\server\share1\dir1\dir2\file.txt` Da qualsiasi indirizzo IP. Il filtro utilizza un percorso completo per `-path` opzione. Le tracce del filtro consentono e negano gli eventi:

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                                 Vserver: vs1
                            Filter Index: 1
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                      Windows User Name: -
                         UNIX User Name: -
                     Trace Allow Events: yes
                         Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

Eliminare i filtri di traccia di sicurezza

Quando non è più necessario un filtro di traccia di protezione, è possibile eliminarlo. Poiché è possibile disporre di un massimo di 10 filtri di traccia di sicurezza per macchina virtuale di storage (SVM), l'eliminazione dei filtri non necessari consente di creare nuovi filtri se si è raggiunto il massimo.

A proposito di questa attività

Per identificare in modo univoco il filtro di traccia di protezione che si desidera eliminare, è necessario specificare quanto segue:

- Il nome della SVM a cui viene applicato il filtro di traccia
- Il numero dell'indice del filtro di traccia

Fasi

1. Identificare il numero di indice del filtro della voce di Security trace filter che si desidera eliminare:

   ```
   vserver security trace filter show -vserver vserver_name

   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        1    -            /dir1/dir2/file.txt          yes      -
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

2. Utilizzando le informazioni sul numero di indice del filtro del passaggio precedente, eliminare la voce del filtro:

```
vserver security trace filter delete -vserver vserver_name -index index_number

vserver security trace filter delete -vserver vs1 -index 1
```

3. Verificare che la voce Security trace filter sia stata eliminata:

```
vserver security trace filter show -vserver vserver_name

vserver security trace filter show -vserver vs1
```

```
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

Eliminare i record di traccia di sicurezza

Dopo aver utilizzato un record di traccia del filtro per verificare la sicurezza dell'accesso ai file o per risolvere i problemi di accesso al client SMB o NFS, è possibile eliminare il record di traccia della protezione dal registro di traccia della protezione.

A proposito di questa attività

Prima di eliminare un record di traccia di protezione, è necessario conoscere il numero di sequenza del record.

> Ogni macchina virtuale di storage (SVM) può memorizzare un massimo di 128 record di traccia. Se si raggiunge il valore massimo sulla SVM, i record di traccia meno recenti vengono eliminati automaticamente quando vengono aggiunti nuovi record. Se non si desidera eliminare manualmente i record di traccia su questa SVM, è possibile consentire a ONTAP di eliminare automaticamente i risultati di traccia meno recenti una volta raggiunto il numero massimo di risultati per creare spazio per i nuovi risultati.

Fasi

1. Identificare il numero di sequenza del record che si desidera eliminare:

```
vserver security trace trace-result show -vserver vserver_name -instance
```

2. Eliminare il record di traccia di protezione:

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name -seqnum integer

vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
999
```

   - `-node node_name` è il nome del nodo del cluster in cui si è verificato l'evento di tracciamento delle autorizzazioni che si desidera eliminare.

Questo è un parametro obbligatorio.

- `-vserver vserver_name` È il nome della SVM in cui si è verificato l'evento di tracciamento delle autorizzazioni che si desidera eliminare.

  Questo è un parametro obbligatorio.

- `-seqnum integer` è il numero di sequenza dell'evento di log che si desidera eliminare.

  Questo è un parametro obbligatorio.

Eliminare tutti i record di traccia di sicurezza

Se non si desidera conservare alcun record di traccia di protezione esistente, è possibile eliminare tutti i record di un nodo con un singolo comando.

Fase

1. Eliminare tutti i record di traccia di sicurezza:

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name *
   ```

   - `-node node_name` è il nome del nodo del cluster in cui si è verificato l'evento di tracciamento delle autorizzazioni che si desidera eliminare.
   - `-vserver vserver_name` È il nome della macchina virtuale di storage (SVM) su cui si è verificato l'evento di tracciamento delle autorizzazioni che si desidera eliminare.

Interpretare i risultati della traccia di sicurezza

I risultati della traccia di protezione forniscono il motivo per cui una richiesta è stata consentita o negata. L'output visualizza il risultato come combinazione del motivo per cui l'accesso è consentito o negato e della posizione all'interno del percorso di controllo degli accessi in cui l'accesso è consentito o negato. È possibile utilizzare i risultati per isolare e identificare i motivi per cui le azioni sono o non sono consentite.

Ricerca di informazioni sugli elenchi dei tipi di risultati e sui dettagli dei filtri

È possibile trovare gli elenchi dei tipi di risultati e i dettagli dei filtri che possono essere inclusi nei risultati della traccia di protezione nelle pagine man di `vserver security trace trace-result show` comando.

Esempio di output da `Reason` in un campo `Allow` tipo di risultato

Di seguito viene riportato un esempio dell'output di `Reason` che viene visualizzato nel log dei risultati della traccia in un `Allow` tipo di risultato:

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

Esempio di output da `Reason` in un campo `Allow` tipo di risultato

Di seguito viene riportato un esempio dell'output di `Reason` che viene visualizzato nel log dei risultati della traccia in un `Deny` tipo di risultato:

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

Esempio di output da `Filter details` campo

Di seguito viene riportato un esempio dell'output di `Filter details` nel log dei risultati della traccia, che elenca lo stile di sicurezza effettivo del file system contenente file e cartelle che corrispondono ai criteri di filtro:

```
Security Style: MIXED and ACL
```

Dove trovare ulteriori informazioni

Una volta verificato l'accesso al client SMB, è possibile eseguire una configurazione SMB avanzata o aggiungere l'accesso SAN. Una volta verificato l'accesso al client NFS, è possibile eseguire una configurazione NFS avanzata o aggiungere l'accesso SAN. Una volta completato l'accesso al protocollo, è necessario proteggere il volume root di SVM.

Configurazione SMB

È possibile configurare ulteriormente l'accesso SMB utilizzando quanto segue:

- "Gestione delle PMI"

  Descrive come configurare e gestire l'accesso ai file utilizzando il protocollo SMB.

- "Report tecnico di NetApp 4191: Guida alle Best practice per i file service Windows di Clustered Data ONTAP 8.2"

  Fornisce una breve panoramica dell'implementazione SMB e di altre funzionalità di servizi file Windows con consigli e informazioni di base per la risoluzione dei problemi di ONTAP.

- "Report tecnico di NetApp 3740: Protocollo CIFS di prossima generazione per PMI 2 in Data ONTAP"

  Descrive le funzionalità di SMB 2, i dettagli di configurazione e la relativa implementazione in ONTAP.

Configurazione NFS

È possibile configurare ulteriormente l'accesso NFS utilizzando quanto segue:

- "Gestione NFS"

Descrive come configurare e gestire l'accesso ai file utilizzando il protocollo NFS.

- "Report tecnico di NetApp 4067: Guida all'implementazione e alle Best practice di NFS"

  Funge da guida operativa NFSv3 e NFSv4 e fornisce una panoramica del sistema operativo ONTAP con particolare attenzione a NFSv4.

- "Report tecnico di NetApp 4668: Guida alle Best practice per i servizi di nome"

  Fornisce un elenco completo di Best practice, limiti, raccomandazioni e considerazioni per la configurazione di LDAP, NIS, DNS e file di utenti e gruppi locali a scopo di autenticazione.

- "Report tecnico NetApp 4616: NFS Kerberos in ONTAP con Microsoft Active Directory"
- "Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP"
- "Report tecnico di NetApp 3580: Guida ai miglioramenti e alle Best practice di NFSv4 per l'implementazione di Data ONTAP"

  Descrive le Best practice da seguire durante l'implementazione dei componenti NFSv4 su client AIX, Linux o Solaris collegati a sistemi che eseguono ONTAP.

Protezione del volume root

Dopo aver configurato i protocolli su SVM, assicurarsi che il volume root sia protetto:

- "Protezione dei dati"

  Descrive come creare un mirror di condivisione del carico per proteggere il volume root SVM, una Best practice NetApp per le SVM abilitate per NAS. Viene inoltre descritto come eseguire rapidamente il ripristino da guasti o perdite di volume promuovendo il volume root SVM da un mirror di condivisione del carico.

Gestione della crittografia con System Manager

Crittografare i dati memorizzati utilizzando la crittografia basata su software

Utilizzare la crittografia del volume per garantire che i dati del volume non possano essere letti se il dispositivo sottostante viene riassegnato, restituito, smarrito o rubato. La crittografia dei volumi non richiede dischi speciali, ma funziona con tutti gli HDD e gli SSD.

La crittografia del volume richiede un gestore delle chiavi. È possibile configurare Onboard Key Manager utilizzando System Manager. È anche possibile utilizzare un gestore di chiavi esterno, ma è necessario prima impostarlo utilizzando l'interfaccia utente di ONTAP.

Una volta configurato il gestore delle chiavi, i nuovi volumi vengono crittografati per impostazione predefinita.

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. In **Encryption**, fare clic su ⚙ Per configurare Onboard Key Manager per la prima volta.
3. Per crittografare i volumi esistenti, fare clic su **Storage > Volumes** (archiviazione > volumi).

4. Sul volume desiderato, fare clic su ⋮ Quindi fare clic su **Edit** (Modifica).
5. Selezionare **Enable Encryption** (attiva crittografia).

Crittografare i dati memorizzati utilizzando unità con crittografia automatica

Utilizzare la crittografia del disco per garantire che tutti i dati di un Tier locale non possano essere letti se il dispositivo sottostante viene riassegnato, restituito, smarrito o rubato. La crittografia dei dischi richiede speciali HDD o SSD con crittografia automatica.

La crittografia del disco richiede un gestore delle chiavi. È possibile configurare il gestore delle chiavi integrato utilizzando System Manager. È anche possibile utilizzare un gestore di chiavi esterno, ma è necessario prima impostarlo utilizzando l'interfaccia utente di ONTAP.

Se ONTAP rileva dischi con crittografia automatica, richiede di configurare il gestore delle chiavi integrato quando si crea il Tier locale.

Fasi

1. In **Encryption**, fare clic su ⚙ per configurare il gestore delle chiavi integrato.
2. Se viene visualizzato un messaggio che indica la necessità di riscrivere i dischi, fare clic su ⋮, Quindi fare clic su **Rekey Disks**.

Gestire la crittografia con la CLI

Panoramica sulla crittografia NetApp

NetApp offre tecnologie di crittografia basate su software e hardware per garantire che i dati inattivi non possano essere letti in caso di riposizionamento, restituzione, smarrimento o furto del supporto di storage.

- La crittografia basata su software con NetApp Volume Encryption (NVE) supporta la crittografia dei dati di un volume alla volta
- La crittografia basata su hardware con NetApp Storage Encryption (NSE) supporta la crittografia completa dei dati su disco (FDE) durante la scrittura.

Configurare NetApp Volume Encryption

Panoramica sulla configurazione di NetApp Volume Encryption

NetApp Volume Encryption (NVE) è una tecnologia software per la crittografia dei dati inattivi di un volume alla volta. Una chiave di crittografia accessibile solo al sistema di storage impedisce la lettura dei dati del volume in caso di riallocazione, restituzione, smarrimento o furto del dispositivo sottostante.

Comprensione di NVE

Con NVE, sia i metadati che i dati (incluse le copie Snapshot) vengono crittografati. L'accesso ai dati viene fornito da una chiave XTS-AES-256 univoca, una per volume. Un server di gestione delle chiavi esterno o Onboard Key Manager (OKM) serve le chiavi ai nodi:

- Il server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol). Si consiglia di configurare i server di gestione delle chiavi esterni su un sistema storage diverso dai dati.
- Onboard Key Manager è uno strumento integrato che serve le chiavi ai nodi dello stesso sistema storage dei dati.

A partire da ONTAP 9.7, la crittografia aggregata e del volume è attivata per impostazione predefinita se si dispone di una licenza di crittografia del volume (VE) e si utilizza un gestore di chiavi integrato o esterno. La licenza VE è inclusa con "ONTAP uno". Ogni volta che viene configurato un gestore di chiavi esterno o integrato, viene modificato il modo in cui viene configurata la crittografia dei dati inattivi per aggregati nuovi di zecca e volumi nuovi di zecca. I nuovi aggregati avranno NetApp aggregate Encryption (NAE) abilitato per impostazione predefinita. I volumi nuovi di zecca che non fanno parte di un aggregato NAE avranno NetApp Volume Encryption (NVE) abilitato per impostazione predefinita. Se una macchina virtuale per lo storage dei dati (SVM) viene configurata con un proprio gestore delle chiavi utilizzando la gestione delle chiavi multi-tenant, il volume creato per tale SVM viene configurato automaticamente con NVE.

È possibile attivare la crittografia su un volume nuovo o esistente. NVE supporta la gamma completa di funzionalità per l'efficienza dello storage, tra cui deduplica e compressione. A partire da ONTAP 9.14.1, è possibile Abilitazione di NVE su volumi root SVM esistenti.

> Se si utilizza SnapLock, è possibile attivare la crittografia solo su volumi SnapLock nuovi e vuoti. Non è possibile attivare la crittografia su un volume SnapLock esistente.

È possibile utilizzare NVE su qualsiasi tipo di aggregato (HDD, SSD, ibrido, LUN array), con qualsiasi tipo di RAID e in qualsiasi implementazione ONTAP supportata, incluso ONTAP Select. È inoltre possibile utilizzare NVE con crittografia basata su hardware per "crittografare `ddoppio`" i dati su dischi con crittografia automatica.

Quando NVE è abilitato, anche il core dump è crittografato.

Crittografia a livello di aggregato

Normalmente, a ogni volume crittografato viene assegnata una chiave univoca. Quando il volume viene cancellato, la chiave viene eliminata con esso.

A partire da ONTAP 9.6, è possibile utilizzare la crittografia aggregata NetApp per assegnare le chiavi all'aggregato contenente per i volumi da crittografare. Quando si elimina un volume crittografato, le chiavi dell'aggregato vengono conservate. Le chiavi vengono eliminate se l'intero aggregato viene cancellato.

Se si intende eseguire la deduplica a livello di aggregato inline o in background, è necessario utilizzare la crittografia a livello di aggregato. La deduplica a livello di aggregato non è altrimenti supportata da NVE.

A partire da ONTAP 9.7, la crittografia aggregata e del volume è attivata per impostazione predefinita se si dispone di una licenza di crittografia del volume (VE) e si utilizza un gestore di chiavi integrato o esterno.

I volumi NVE e NAE possono coesistere sullo stesso aggregato. Per impostazione predefinita, i volumi crittografati con crittografia a livello di aggregato sono volumi NAE. È possibile ignorare l'impostazione predefinita quando si crittografa il volume.

È possibile utilizzare `volume move` Per convertire un volume NVE in un volume NAE e viceversa. È possibile replicare un volume NAE in un volume NVE.

Non è possibile utilizzare `secure purge` Comandi su un volume NAE.

Quando utilizzare server di gestione delle chiavi esterni

Sebbene sia meno costoso e generalmente più conveniente utilizzare il gestore delle chiavi integrato, è necessario configurare i server KMIP se si verifica una delle seguenti condizioni:

- La soluzione di gestione delle chiavi di crittografia deve essere conforme agli standard FIPS (Federal Information Processing Standards) 140-2 o ALLO standard OASIS KMIP.
- Hai bisogno di una soluzione multi-cluster, con gestione centralizzata delle chiavi di crittografia.
- La tua azienda richiede una maggiore sicurezza nell'archiviazione delle chiavi di autenticazione su un sistema o in una posizione diversa dai dati.

Scopo della gestione esterna delle chiavi

L'ambito della gestione esterna delle chiavi determina se i server di gestione delle chiavi proteggono tutte le SVM nel cluster o solo le SVM selezionate:

- È possibile utilizzare un *ambito del cluster* per configurare la gestione delle chiavi esterne per tutte le SVM nel cluster. L'amministratore del cluster ha accesso a tutte le chiavi memorizzate sui server.
- A partire da ONTAP 9.6, è possibile utilizzare un *ambito SVM* per configurare la gestione delle chiavi esterne per una SVM denominata nel cluster. Questo è il meglio per gli ambienti multi-tenant in cui ciascun tenant utilizza una SVM (o un insieme di SVM) diversa per la distribuzione dei dati. Solo l'amministratore SVM di un determinato tenant ha accesso alle chiavi del tenant.
- A partire da ONTAP 9.10.1, è possibile utilizzare Azure Key Vault e Google Cloud KMS Proteggere le chiavi NVE solo per dati SVM. Questa funzione è disponibile per i sistemi KMS di AWS a partire dal 9.12.0.

È possibile utilizzare entrambi gli ambiti nello stesso cluster. Se i server di gestione delle chiavi sono stati configurati per una SVM, ONTAP utilizza solo questi server per proteggere le chiavi. In caso contrario, ONTAP protegge le chiavi con i server di gestione delle chiavi configurati per il cluster.

Un elenco di Key Manager esterni validati è disponibile in "Tool di matrice di interoperabilità NetApp (IMT)". Per trovare questo elenco, inserire il termine "Key Manager" nella funzione di ricerca di IMT.

Dettagli del supporto

La seguente tabella mostra i dettagli del supporto NVE:

Risorsa o funzione	Dettagli del supporto
Piattaforme	Funzionalità di offload AES-NI richiesta. Consultare il Hardware Universe (HWU) per verificare che NVE e NAE siano supportati per la piattaforma in uso.

Crittografia	A partire da ONTAP 9.7, gli aggregati e i volumi appena creati vengono crittografati per impostazione predefinita quando si aggiunge una licenza VE (Volume Encryption) e si dispone di un gestore di chiavi integrato o esterno configurato. Se è necessario creare un aggregato non crittografato, utilizzare il seguente comando:
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	Se è necessario creare un volume di testo normale, utilizzare il seguente comando:
	
	`volume create -encrypt false`
	
	La crittografia non è attivata per impostazione predefinita quando:
	
	• La licenza VE non è installata.
	• Gestore chiavi non configurato.
	• La piattaforma o il software non supportano la crittografia.
	• La crittografia hardware è attivata.

ONTAP	Tutte le implementazioni ONTAP. Il supporto per il cloud ONTAP è disponibile in ONTAP 9.5 e versioni successive.
Dispositivi	HDD, SSD, ibrido, LUN array.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
Volumi	Volumi di dati e volumi root della SVM esistenti. Non puoi crittografare i dati sui volumi di metadati MetroCluster. Nelle versioni di ONTAP precedenti alla 9.14.1, non è possibile crittografare i dati sul volume root della SVM con NVE. A partire da ONTAP 9.14.1, ONTAP supporta NVE su volumi root SVM.
Crittografia a livello di aggregato	A partire da ONTAP 9.6, NVE supporta la crittografia a livello aggregato (NAE): • Se si intende eseguire la deduplica a livello di aggregato inline o in background, è necessario utilizzare la crittografia a livello di aggregato. • Non è possibile reimmettere la chiave di un volume di crittografia a livello di aggregato. • L'eliminazione sicura non è supportata sui volumi di crittografia a livello di aggregato. • Oltre ai volumi di dati, NAE supporta la crittografia dei volumi root SVM e del volume di metadati MetroCluster. NAE non supporta la crittografia del volume root.
Ambito SVM	A partire da ONTAP 9.6, NVE supporta l'ambito SVM solo per la gestione delle chiavi esterne, non per Onboard Key Manager. MetroCluster è supportato a partire da ONTAP 9.8.

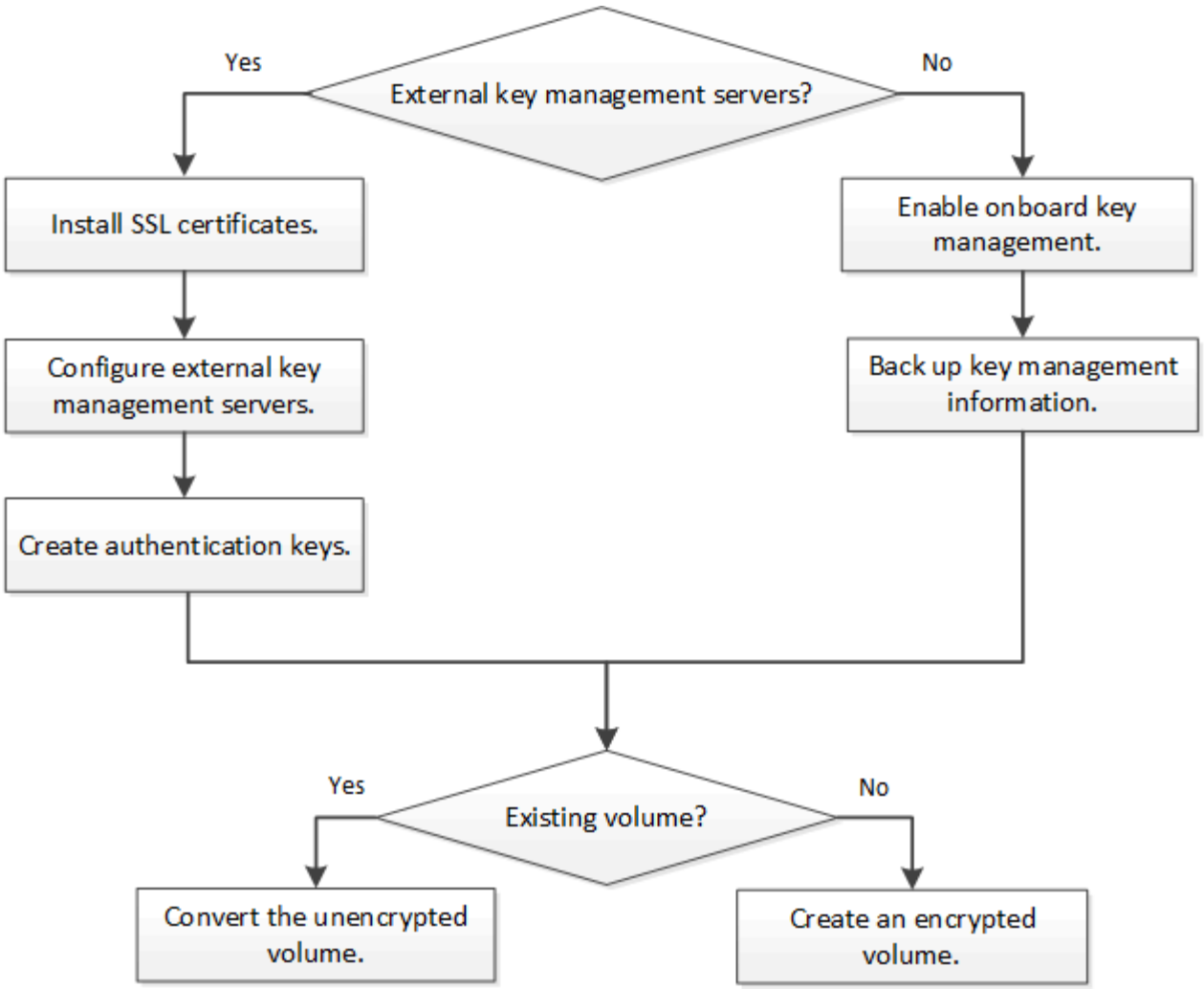
Efficienza dello storage	Deduplica, compressione, compattazione, FlexClone. I cloni utilizzano la stessa chiave del padre, anche dopo aver sdoppiato il clone dal padre. Eseguire una `volume move` su un clone split, dopodiché il clone split avrà una chiave diversa.
Replica	• Per la replica dei volumi, i volumi di origine e di destinazione possono avere impostazioni di crittografia diverse. La crittografia può essere configurata per l'origine e non configurata per la destinazione e viceversa. • Per la replica SVM, il volume di destinazione viene crittografato automaticamente, a meno che la destinazione non contenga un nodo che supporti la crittografia del volume, nel qual caso la replica riesce, ma il volume di destinazione non viene crittografato. • Per le configurazioni MetroCluster, ogni cluster estrae le chiavi di gestione delle chiavi esterne dai relativi server delle chiavi configurati. Le chiavi OKM vengono replicate nel sito del partner dal servizio di replica della configurazione.
Conformità	A partire da ONTAP 9.2, SnapLock è supportato sia in modalità Compliance che Enterprise, solo per nuovi volumi. Non è possibile attivare la crittografia su un volume SnapLock esistente.
FlexGroups	A partire da ONTAP 9.2, sono supportati FlexGroups. Gli aggregati di destinazione devono essere dello stesso tipo degli aggregati di origine, a livello di volume o aggregato. A partire da ONTAP 9.5, è supportata la rekey in-place dei volumi FlexGroup.
Transizione 7-Mode	A partire da 7-Mode Transition Tool 3.3, è possibile utilizzare 7-Mode Transition Tool CLI per eseguire una transizione basata su copia a volumi di destinazione abilitati per NVE sul sistema in cluster.

Informazioni correlate

"FAQ - NetApp Volume Encryption e NetApp aggregate Encryption"

Workflow di NetApp Volume Encryption

È necessario configurare i servizi di gestione delle chiavi prima di poter attivare la crittografia dei volumi. È possibile attivare la crittografia su un nuovo volume o su un volume esistente.



"È necessario installare la licenza VE" E configurare i servizi di gestione delle chiavi prima di poter criptare i dati con NVE. Prima di installare la licenza, è necessario "Determinare se la versione di ONTAP in uso supporta NVE".

Configurare NVE

Determinare se la versione del cluster supporta NVE

Prima di installare la licenza, è necessario determinare se la versione del cluster supporta NVE. È possibile utilizzare `version` per determinare la versione del cluster.

A proposito di questa attività

La versione del cluster è la versione più bassa di ONTAP in esecuzione su qualsiasi nodo del cluster.

Fase

1. Determinare se la versione del cluster supporta NVE:

   ```
   version -v
   ```

   NVE non è supportato se l'output del comando visualizza il testo "1Ono-DARE" (per "no Data at Rest Encryption") o se si utilizza una piattaforma non elencata nella "Dettagli del supporto".

   Il seguente comando determina se NVE è supportato su `cluster1`.

```
cluster1::> version -v
NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
```

L'output di `1Ono-DARE` Indica che NVE non è supportato sulla versione del cluster.

Installare la licenza

Una licenza VE consente di utilizzare la funzione su tutti i nodi del cluster. Questa licenza è necessaria prima di poter crittografare i dati con NVE. È incluso con "ONTAP uno".

Prima di ONTAP One, la licenza VE era inclusa nel pacchetto crittografia. Il pacchetto di crittografia non è più disponibile, ma è ancora valido. Sebbene non sia attualmente richiesto, i clienti esistenti possono scegliere di farlo "Eseguire l'aggiornamento a ONTAP One".

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario aver ricevuto la chiave di licenza VE dal rappresentante di vendita o avere installato ONTAP ONE.

Fasi

1. "Verificare che la licenza VE sia installata".

   Il nome del pacchetto di licenza VE è `VE`.

2. Se la licenza non è installata, "Utilizzare Gestione sistema o l'interfaccia CLI di ONTAP per installarlo".

Configurare la gestione esterna delle chiavi

Configurare una panoramica sulla gestione esterna delle chiavi

È possibile utilizzare uno o più server di gestione delle chiavi esterni per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. Un server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol).

> Per ONTAP 9.1 e versioni precedenti, è necessario assegnare le LIF di gestione dei nodi alle porte configurate con il ruolo di gestione dei nodi prima di poter utilizzare il gestore delle chiavi esterno.

NetApp Volume Encryption (NVE) supporta Onboard Key Manager in ONTAP 9.1 e versioni successive. A partire da ONTAP 9.3, NVE supporta la gestione delle chiavi esterne (KMIP) e Onboard Key Manager. A partire da ONTAP 9.10.1, è possibile utilizzare Azure Key Vault o Google Cloud Key Manager Service Per proteggere le chiavi NVE. A partire da ONTAP 9.11.1, è possibile configurare più Key Manager esterni in un cluster. Vedere Configurare i server delle chiavi in cluster.

Gestisci i manager delle chiavi esterne con System Manager

A partire da ONTAP 9.7, è possibile memorizzare e gestire le chiavi di autenticazione e crittografia con Onboard Key Manager. A partire da ONTAP 9.13.1, è possibile utilizzare

anche i gestori delle chiavi esterni per memorizzare e gestire queste chiavi.

Onboard Key Manager memorizza e gestisce le chiavi in un database sicuro interno al cluster. Il suo scopo è il cluster. Un gestore delle chiavi esterno memorizza e gestisce le chiavi all'esterno del cluster. Il suo ambito può essere il cluster o la VM di storage. È possibile utilizzare uno o più gestori di chiavi esterne. Si applicano le seguenti condizioni:

- Se Onboard Key Manager è attivato, non è possibile attivare un gestore di chiavi esterno a livello di cluster, ma può essere attivato a livello di storage VM.
- Se un gestore delle chiavi esterno è abilitato a livello di cluster, il gestore delle chiavi integrato non può essere abilitato.

Quando si utilizzano key manager esterni, è possibile registrare fino a quattro key server primari per storage VM e cluster. Ogni server principale delle chiavi può essere cluster con un massimo di tre server secondari delle chiavi.

Configurare un gestore di chiavi esterno

Per aggiungere un gestore di chiavi esterno per una VM di storage, è necessario aggiungere un gateway opzionale quando si configura l'interfaccia di rete per la VM di storage. Se la VM di storage è stata creata senza il percorso di rete, sarà necessario creare il percorso in modo esplicito per il gestore delle chiavi esterno. Vedere "Creazione di una LIF (interfaccia di rete)".

Fasi

È possibile configurare un gestore di chiavi esterno partendo da posizioni diverse in System Manager.

1. Per configurare un gestore di chiavi esterno, eseguire una delle seguenti operazioni iniziali.

Workflow	Navigazione	Fase di avvio
Configurare Key Manager	**Cluster** > **Impostazioni**	Scorrere fino alla sezione **sicurezza**. In **Encryption**, selezionare ⚙. Selezionare **External Key Manager**.
Aggiungi Tier locale	**Storage** > **Tier**	Selezionare **+ Aggiungi livello locale**. Selezionare la casella di controllo "Configure Key Manager" (Configura gestore chiavi). Selezionare **External Key Manager**.
Preparare lo storage	**Dashboard**	Nella sezione **capacità**, selezionare **Prepare Storage** (prepara storage). Quindi, selezionare "Configure Key Manager" (Configura gestore chiavi). Selezionare **External Key Manager**.
Configurare la crittografia (solo gestore delle chiavi nell'ambito delle macchine virtuali di storage)	**Storage** > **Storage VM**	Selezionare la VM di storage. Selezionare la scheda **Impostazioni**. Nella sezione **Encryption** sotto **Security**, selezionare ⚙.

2. Per aggiungere un server delle chiavi principale, selezionare + Add E compilare i campi **IP Address (Indirizzo IP) o host Name (Nome host)** e **Port** (porta).

3. I certificati esistenti installati sono elencati nei campi **certificati CA del server KMIP** e **certificato client KMIP**. È possibile eseguire una delle seguenti operazioni:
   - Selezionare ⌄ per selezionare i certificati installati che si desidera mappare al gestore delle chiavi. (È possibile selezionare più certificati CA di servizio, ma è possibile selezionare un solo certificato client).
   - Selezionare **Aggiungi nuovo certificato** per aggiungere un certificato non ancora installato e associarlo al gestore delle chiavi esterno.
   - Selezionare × accanto al nome del certificato per eliminare i certificati installati che non si desidera mappare al gestore delle chiavi esterno.
4. Per aggiungere un server chiavi secondario, selezionare **Aggiungi** nella colonna **Server chiavi secondari** e fornire i relativi dettagli.
5. Selezionare **Salva** per completare la configurazione.

Modificare un gestore di chiavi esterno esistente

Se è già stato configurato un gestore di chiavi esterno, è possibile modificarne le impostazioni.

Fasi

1. Per modificare la configurazione di un gestore di chiavi esterno, eseguire una delle seguenti operazioni iniziali.

Scopo	Navigazione	Fase di avvio
Gestore delle chiavi esterne dell'ambito del cluster	**Cluster** > **Impostazioni**	Scorrere fino alla sezione **sicurezza**. In **Encryption**, selezionare ⋮, Quindi selezionare **Edit External Key Manager** (Modifica gestore chiavi esterno).
Storage VM Scope External Key Manager	**Storage** > **Storage VM**	Selezionare la VM di storage. Selezionare la scheda **Impostazioni**. Nella sezione **Encryption** sotto **Security**, selezionare ⋮, Quindi selezionare **Edit External Key Manager** (Modifica gestore chiavi esterno).

2. I server delle chiavi esistenti sono elencati nella tabella **Server delle chiavi**. È possibile eseguire le seguenti operazioni:
   - Aggiungere un nuovo server chiavi selezionando + Add .
   - Eliminare un server delle chiavi selezionando ⋮ alla fine della cella della tabella che contiene il nome del server delle chiavi. Anche i server di chiavi secondari associati a quel server di chiavi primario vengono rimossi dalla configurazione.

Eliminare un gestore di chiavi esterno

Se i volumi non sono crittografati, è possibile eliminare un gestore di chiavi esterno.

Fasi

1. Per eliminare un gestore di chiavi esterno, eseguire una delle seguenti operazioni.

Scopo	Navigazione	Fase di avvio

Gestore delle chiavi esterne dell'ambito del cluster	**Cluster** > **Impostazioni**	Scorrere fino alla sezione **sicurezza**. In **Encryption**, selezionare ⋮, Quindi selezionare **Delete External Key Manager** (Elimina gestore chiavi esterne).
Storage VM Scope External Key Manager	**Storage** > **Storage VM**	Selezionare la VM di storage. Selezionare la scheda **Impostazioni**. Nella sezione **Encryption** sotto **Security**, selezionare ⋮, Quindi selezionare **Delete External Key Manager** (Elimina gestore chiavi esterne).

Migrare le chiavi tra i principali manager

Quando su un cluster sono attivati più gestori di chiavi, è necessario migrare le chiavi da un gestore di chiavi a un altro. Questo processo viene completato automaticamente con System Manager.

- Se Onboard Key Manager o un gestore di chiavi esterno è abilitato a livello di cluster e alcuni volumi sono crittografati, Quindi, quando si configura un gestore di chiavi esterno a livello di storage VM, le chiavi devono essere migrate da Onboard Key Manager o da un gestore di chiavi esterno a livello di cluster a un gestore di chiavi esterno a livello di storage VM. Questo processo viene completato automaticamente da System Manager.
- Se i volumi sono stati creati senza crittografia su una VM di storage, non è necessario migrare le chiavi.

Installare i certificati SSL sul cluster

Il cluster e il server KMIP utilizzano i certificati SSL KMIP per verificare l'identità reciproca e stabilire una connessione SSL. Prima di configurare la connessione SSL con il server KMIP, è necessario installare i certificati SSL del client KMIP per il cluster e il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.

A proposito di questa attività

In una coppia ha, entrambi i nodi devono utilizzare gli stessi certificati SSL KMIP pubblici e privati. Se si collegano più coppie ha allo stesso server KMIP, tutti i nodi delle coppie ha devono utilizzare gli stessi certificati SSL KMIP pubblici e privati.

Prima di iniziare

- L'ora deve essere sincronizzata sul server che crea i certificati, sul server KMIP e sul cluster.
- È necessario avere ottenuto il certificato del client KMIP SSL pubblico per il cluster.
- È necessario aver ottenuto la chiave privata associata al certificato del client SSL KMIP per il cluster.
- Il certificato del client SSL KMIP non deve essere protetto da password.
- È necessario aver ottenuto il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.
- In un ambiente MetroCluster, è necessario installare gli stessi certificati SSL KMIP su entrambi i cluster.

> È possibile installare i certificati client e server sul server KMIP prima o dopo l'installazione dei certificati sul cluster.

Fasi

1. Installare i certificati del client KMIP SSL per il cluster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   Viene richiesto di immettere i certificati SSL KMIP pubblici e privati.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Installare il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP:

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Abilitare la gestione esterna delle chiavi in ONTAP 9.6 e versioni successive (NVE)

È possibile utilizzare uno o più server KMIP per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. A partire da ONTAP 9.6, è possibile configurare un gestore di chiavi esterno separato per proteggere le chiavi utilizzate da un SVM di dati per accedere ai dati crittografati.

A partire da ONTAP 9.11.1, è possibile aggiungere fino a 3 server chiavi secondari per server chiavi primario per creare un server chiavi in cluster. Per ulteriori informazioni, vedere Configurare i server di chiavi esterne in cluster.

A proposito di questa attività

È possibile collegare fino a quattro server KMIP a un cluster o a una SVM. Si consiglia di utilizzare almeno due server per la ridondanza e il disaster recovery.

L'ambito della gestione esterna delle chiavi determina se i server di gestione delle chiavi proteggono tutte le SVM nel cluster o solo le SVM selezionate:

- È possibile utilizzare un *ambito del cluster* per configurare la gestione delle chiavi esterne per tutte le SVM nel cluster. L'amministratore del cluster ha accesso a tutte le chiavi memorizzate sui server.
- A partire da ONTAP 9.6, è possibile utilizzare un *ambito SVM* per configurare la gestione delle chiavi esterne per una SVM di dati nel cluster. Questo è il meglio per gli ambienti multi-tenant in cui ciascun tenant utilizza una SVM (o un insieme di SVM) diversa per la distribuzione dei dati. Solo l'amministratore SVM di un determinato tenant ha accesso alle chiavi del tenant.
- Per gli ambienti multi-tenant, installare una licenza per *MT_EK_MGMT* utilizzando il seguente comando:

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

  Per la sintassi completa dei comandi, vedere la pagina man del comando.

È possibile utilizzare entrambi gli ambiti nello stesso cluster. Se i server di gestione delle chiavi sono stati configurati per una SVM, ONTAP utilizza solo questi server per proteggere le chiavi. In caso contrario, ONTAP protegge le chiavi con i server di gestione delle chiavi configurati per il cluster.

È possibile configurare la gestione delle chiavi integrata nell'ambito del cluster e la gestione delle chiavi esterne nell'ambito SVM. È possibile utilizzare `security key-manager key migrate` Comando per la migrazione delle chiavi dalla gestione delle chiavi integrata nell'ambito del cluster ai key manager esterni

nell'ambito SVM.

Prima di iniziare

- I certificati del server e del client SSL KMIP devono essere stati installati.
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- Se si desidera attivare la gestione esterna delle chiavi per un ambiente MetroCluster, MetroCluster deve essere completamente configurato prima di attivare la gestione esterna delle chiavi.
- In un ambiente MetroCluster, è necessario installare il certificato SSL KMIP su entrambi i cluster.

Fasi

1. Configurare la connettività del gestore delle chiavi per il cluster:

   `security key-manager external enable -vserver admin_SVM -key-servers host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert server_CA_certificates`

   - Il `security key-manager external enable` il comando sostituisce `security key-manager setup` comando. Se si esegue il comando al prompt di login del cluster, *`admin_SVM`* Per impostazione predefinita, viene impostata la SVM amministrativa del cluster corrente. Per configurare l'ambito del cluster, è necessario essere l'amministratore del cluster. È possibile eseguire `security key-manager external modify` comando per modificare la configurazione di gestione delle chiavi esterne.
   - In un ambiente MetroCluster, se si sta configurando la gestione esterna delle chiavi per la SVM amministrativa, è necessario ripetere `security key-manager external enable` sul cluster partner.

   Il seguente comando abilita la gestione esterna delle chiavi per `cluster1` con tre key server esterni. Il primo server chiavi viene specificato utilizzando il nome host e la porta, il secondo viene specificato utilizzando un indirizzo IP e la porta predefinita, mentre il terzo viene specificato utilizzando un indirizzo IPv6 e una porta:

   ```
   cluster1::> security key-manager external enable -vserver cluster1 -key
   -servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. Configurare un gestore delle chiavi e una SVM:

   `security key-manager external enable -vserver SVM -key-servers host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert server_CA_certificates`

- Se si esegue il comando al prompt di accesso SVM, `SVM` Per impostazione predefinita, viene impostata la SVM corrente. Per configurare l'ambito di SVM, è necessario essere un amministratore del cluster o di SVM. È possibile eseguire `security key-manager external modify` comando per modificare la configurazione di gestione delle chiavi esterne.
- In un ambiente MetroCluster, se si configura la gestione esterna delle chiavi per una SVM di dati, non è necessario ripetere `security key-manager external enable` sul cluster partner.

Il seguente comando abilita la gestione esterna delle chiavi per `svm1` con un server a chiave singola in ascolto sulla porta predefinita 5696:

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. Ripetere l'ultimo passaggio per eventuali SVM aggiuntive.

È inoltre possibile utilizzare `security key-manager external add-servers` Comando per configurare SVM aggiuntive. Il `security key-manager external add-servers` il comando sostituisce `security key-manager add` comando. Per la sintassi completa dei comandi, vedere la pagina man.

4. Verificare che tutti i server KMIP configurati siano connessi:

```
security key-manager external show-status -node node_name
```

Il `security key-manager external show-status` il comando sostituisce `security key-manager show -status` comando. Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ----------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available
node2
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available

8 entries were displayed.
```

5. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

   `volume encryption conversion start`

   Prima di convertire i volumi, è necessario configurare completamente un gestore di chiavi esterno. In un ambiente MetroCluster, è necessario configurare un gestore di chiavi esterno su entrambi i siti.

Abilitare la gestione esterna delle chiavi in ONTAP 9.5 e versioni precedenti

È possibile utilizzare uno o più server KMIP per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È possibile collegare fino a quattro server KMIP a un nodo. Si consiglia di utilizzare almeno due server per la ridondanza e il disaster recovery.

A proposito di questa attività

ONTAP configura la connettività del server KMIP per tutti i nodi del cluster.

Prima di iniziare

- I certificati del server e del client SSL KMIP devono essere stati installati.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare un gestore di chiavi esterno.
- In un ambiente MetroCluster, è necessario installare il certificato SSL KMIP su entrambi i cluster.

Fasi

1. Configurare la connettività del gestore delle chiavi per i nodi del cluster:

```
security key-manager setup
```

Viene avviata la configurazione di Key Manager.

> In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

2. Immettere la risposta appropriata a ogni richiesta.
3. Aggiunta di un server KMIP:

```
security key-manager add -address key_management_server_ipaddress
```

```
clusterl::> security key-manager add -address 20.1.1.1
```

> In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

4. Aggiungere un server KMIP aggiuntivo per la ridondanza:

```
security key-manager add -address key_management_server_ipaddress
```

```
clusterl::> security key-manager add -address 20.1.1.2
```

> In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

5. Verificare che tutti i server KMIP configurati siano connessi:

```
security key-manager show -status
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> security key-manager show -status

Node            Port      Registered Key Manager  Status
--------------  ----      ----------------------  ---------------
cluster1-01     5696      20.1.1.1                available
cluster1-01     5696      20.1.1.2                available
cluster1-02     5696      20.1.1.1                available
cluster1-02     5696      20.1.1.2                available
```

6. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

```
volume encryption conversion start
```

Prima di convertire i volumi, è necessario configurare completamente un gestore di chiavi esterno. In un ambiente MetroCluster, è necessario configurare un gestore di chiavi esterno su entrambi i siti.

Gestire le chiavi con un cloud provider

A partire da ONTAP 9.10.1, è possibile utilizzare "Azure Key Vault (AKV)" e. "Servizio di gestione delle chiavi di Google Cloud Platform (Cloud KMS)" Per proteggere le chiavi di crittografia ONTAP in un'applicazione ospitata nel cloud. A partire da ONTAP 9.12.0, è anche possibile proteggere le chiavi NVE con "KMS DI AWS".

AWS KMS, AKV e Cloud KMS possono essere utilizzati per proteggere "Chiavi NetApp Volume Encryption (NVE)" Solo per SVM di dati.

A proposito di questa attività

La gestione delle chiavi con un provider cloud può essere abilitata con l'interfaccia CLI o l'API REST ONTAP.

Quando si utilizza un cloud provider per proteggere le chiavi, tenere presente che per impostazione predefinita viene utilizzata una LIF SVM dati per comunicare con l'endpoint di gestione delle chiavi cloud. Una rete di gestione dei nodi viene utilizzata per comunicare con i servizi di autenticazione del provider cloud (login.microsoftonline.com per Azure; oauth2.googleapis.com per Cloud KMS). Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

Quando si utilizza un servizio di gestione delle chiavi di un provider cloud, è necessario tenere presenti le seguenti limitazioni:

- La gestione delle chiavi con cloud provider non è disponibile per crittografia dello storage NetApp (NSE) e crittografia aggregata di NetApp (NAE). "KMIP esterni" può essere utilizzato in alternativa.
- La gestione delle chiavi del provider cloud non è disponibile per le configurazioni MetroCluster.
- La gestione delle chiavi del cloud provider può essere configurata solo su una SVM dati.

Prima di iniziare

- È necessario aver configurato il KMS sul cloud provider appropriato.
- I nodi del cluster ONTAP devono supportare NVE.
- "È necessario aver installato le licenze Volume Encryption (VE) e Encryption Key Management (MTEKM) multi-tenant". Queste licenze sono incluse con "ONTAP uno".
- Devi essere un amministratore del cluster o di SVM.
- I dati SVM non devono includere volumi crittografati né utilizzare un gestore delle chiavi. Se i dati SVM includono volumi crittografati, è necessario eseguirne la migrazione prima di configurare il KMS.

Abilitare la gestione esterna delle chiavi

L'attivazione della gestione esterna delle chiavi dipende dal gestore specifico delle chiavi utilizzato. Scegliere la scheda del gestore delle chiavi e dell'ambiente appropriati.

AWS

Prima di iniziare

- È necessario creare una concessione per la chiave AWS KMS che verrà utilizzata dal ruolo IAM che gestisce la crittografia. Il ruolo IAM deve includere una policy che consenta le seguenti operazioni:
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`

    Per ulteriori informazioni, consultare la documentazione AWS per "sovvenzioni".

Abilitare AWS KMV su una SVM ONTAP

1. Prima di iniziare, procurarsi l'ID della chiave di accesso e la chiave segreta da AWS KMS.
2. Impostare il livello di privilegio su Advanced (avanzato):
   `set -priv advanced`
3. Abilitare AWS KMS:
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Quando richiesto, inserire la chiave segreta.
5. Verificare che AWS KMS sia stato configurato correttamente:
   `security key-manager external aws show -vserver` *`svm_name`*

Azure

Abilitare il vault delle chiavi Azure su una SVM ONTAP

1. Prima di iniziare, è necessario ottenere le credenziali di autenticazione appropriate dall'account Azure, un certificato o un segreto client. È inoltre necessario garantire che tutti i nodi del cluster siano integri. Puoi controllare questo con il comando `cluster show`.
2. Impostare il livello di privilegi su avanzato
   `set -priv advanced`
3. Abilitare AKV su SVM
   `security key-manager external azure enable -client-id *client_id* -tenant-id *tenant_id* -name -key-id *key_id* -authentication-method {certificate|client-secret}` Quando richiesto, immettere il certificato del client o il segreto del client dall'account Azure.
4. Verificare che AKV sia attivato correttamente:
   `security key-manager external azure show vserver` *`svm_name`*
   Se la raggiungibilità del servizio non è corretta, stabilire la connettività con il servizio di gestione delle chiavi AKV tramite data SVM LIF.

Google Cloud

Abilitare KMS cloud su una SVM ONTAP

1. Prima di iniziare, ottenere la chiave privata per il file delle chiavi dell'account Google Cloud KMS in formato JSON. Questo è disponibile nel tuo account GCP.
   È inoltre necessario garantire che tutti i nodi del cluster siano integri. Puoi controllare questo con il comando `cluster show`.
2. Impostare il livello di privilegi su avanzato:

```
set -priv advanced
```

3. Abilitare Cloud KMS su SVM
   `security key-manager external gcp enable -vserver svm_name -project-id project_id-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name key_name`
   Quando richiesto, inserire il contenuto del file JSON con la chiave privata dell'account di servizio
4. Verificare che Cloud KMS sia configurato con i parametri corretti:
   `security key-manager external gcp show vserver svm_name`
   Lo stato di `kms_wrapped_key_status` lo sarà `"UNKNOWN"` se non sono stati creati volumi crittografati.
   Se la raggiungibilità del servizio non è corretta, stabilire la connettività al servizio di gestione delle chiavi GCP tramite data SVM LIF.

Se uno o più volumi crittografati sono già configurati per un SVM di dati e le chiavi NVE corrispondenti sono gestite dal gestore delle chiavi integrato SVM di amministrazione, tali chiavi devono essere migrate al servizio di gestione delle chiavi esterno. Per eseguire questa operazione con la CLI, eseguire il comando: `security key-manager key migrate -from-Vserver *admin_SVM* -to-Vserver *data_SVM*` Non è possibile creare nuovi volumi crittografati per i dati SVM del tenant fino a quando tutte le chiavi NVE dei dati SVM non vengono migrate correttamente.

Informazioni correlate

- "Crittografia dei volumi con le soluzioni di crittografia NetApp per Cloud Volumes ONTAP"

Abilitare la gestione delle chiavi integrata in ONTAP 9.6 e versioni successive (NVE)

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

A proposito di questa attività

È necessario eseguire `security key-manager onboard sync` ogni volta che si aggiunge un nodo al cluster.

Se si dispone di una configurazione MetroCluster, è necessario eseguire `security key-manager onboard enable` eseguire prima il comando sul cluster locale, quindi eseguire `security key-manager onboard sync` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi. Quando si esegue `security key-manager onboard enable` dal cluster locale, quindi eseguire la sincronizzazione sul cluster remoto, non è necessario eseguire `enable` comando di nuovo dal cluster remoto.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. È possibile utilizzare `cc-mode-enabled=yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Per NVE, se si imposta `cc-mode-enabled=yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente. Per `volume create`, non è necessario specificare `-encrypt true`. Per `volume move start`, non è necessario specificare `-encrypt-destination true`.

Quando si configura la crittografia dei dati ONTAP a riposo, per soddisfare i requisiti per le soluzioni commerciali per classificati (CSFC), è necessario utilizzare NSE con NVE e assicurarsi che il gestore delle chiavi integrato sia attivato in modalità Criteri comuni. Fare riferimento a. "CSFC Solution Brief" Per ulteriori

informazioni su CSFC.

> Quando Onboard Key Manager è attivato in modalità Common Criteria (Criteri comuni) (`cc-mode-enabled=yes`), il comportamento del sistema viene modificato nei seguenti modi:
>
> - Il sistema monitora i tentativi consecutivi di passphrase del cluster non riusciti quando si opera in modalità Common Criteria.
>
> Se non si riesce a inserire la passphrase del cluster corretta all'avvio, i volumi crittografati non vengono montati. Per risolvere questo problema, riavviare il nodo e inserire la passphrase del cluster corretta. Una volta avviato, il sistema consente fino a 5 tentativi consecutivi di inserire correttamente la passphrase del cluster in un periodo di 24 ore per qualsiasi comando che richieda la passphrase del cluster come parametro. Se il limite viene raggiunto (ad esempio, non è stato possibile inserire correttamente la passphrase del cluster 5 volte di seguito), è necessario attendere che il periodo di timeout di 24 ore sia trascorso oppure riavviare il nodo per ripristinare il limite.
>
> - Gli aggiornamenti delle immagini di sistema utilizzano il certificato di firma del codice NetApp RSA-3072 insieme ai digest con firma del codice SHA-384 per controllare l'integrità dell'immagine invece del certificato di firma del codice NetApp RSA-2048 e dei digest con firma del codice SHA-256.
>
> Il comando upgrade verifica che il contenuto dell'immagine non sia stato alterato o corrotto controllando varie firme digitali. Se la convalida ha esito positivo, il processo di aggiornamento dell'immagine passa alla fase successiva; in caso contrario, l'aggiornamento dell'immagine non riesce. Vedere `cluster image` pagina man per informazioni relative agli aggiornamenti del sistema.

> Onboard Key Manager memorizza le chiavi nella memoria volatile. I contenuti della memoria volatile vengono cancellati quando il sistema viene riavviato o arrestato. In condizioni operative normali, il contenuto della memoria volatile viene cancellato entro 30 secondi quando il sistema viene arrestato.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare il Gestore chiavi integrato.

Fasi

1. Avviare la configurazione di Key Manager:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

> Impostare `cc-mode-enabled=yes` per richiedere agli utenti di inserire la passphrase del gestore delle chiavi dopo un riavvio. Per NVE, se si imposta `cc-mode-enabled=yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente. Il `- cc-mode-enabled` L'opzione non è supportata nelle configurazioni MetroCluster. Il `security key-manager onboard enable` il comando sostituisce `security key-manager setup` comando.

Nell'esempio seguente viene avviato il comando di configurazione del gestore delle chiavi sul cluster1 senza che sia necessario inserire la passphrase dopo ogni riavvio:

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Al prompt della passphrase, immettere una passphrase compresa tra 32 e 256 caratteri oppure, per “cc-mode”, una passphrase compresa tra 64 e 256 caratteri.

> Se la passphrase “cc-mode” specificata è inferiore a 64 caratteri, si verifica un ritardo di cinque secondi prima che l’operazione di configurazione del gestore delle chiavi visualizzi nuovamente il prompt della passphrase.

3. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.
4. Verificare che le chiavi di autenticazione siano state create:

   `security key-manager key query -key-type NSE-AK`

   > Il `security key-manager key query` il comando sostituisce `security key-manager query key` comando. Per la sintassi completa dei comandi, vedere la pagina man.

   Nell’esempio seguente viene verificata la creazione di chiavi di autenticazione per `cluster1`:

```
cluster1::> security key-manager key query -key-type NSE-AK
               Node: node1
            Vserver: cluster1
        Key Manager: onboard
   Key Manager Type: OKM
 Key Manager Policy: -

 Key Tag                                Key Type Encryption   Restored

-----------------------------------  -------- ------------ --------

node1                                 NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                 NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
00000000

2 entries were displayed.
```

5. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

   `volume encryption conversion start`

   Onboard Key Manager deve essere completamente configurato prima di convertire i volumi. In un ambiente MetroCluster, il gestore delle chiavi integrato deve essere configurato su entrambi i siti.

Al termine

Copiare la passphrase in una posizione sicura all'esterno del sistema di storage per utilizzarla in futuro.

Ogni volta che si configura la passphrase di Onboard Key Manager, è necessario eseguire il backup manuale delle informazioni in una posizione sicura all'esterno del sistema di storage per l'utilizzo in caso di disastro. Vedere "Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate".

Abilitare la gestione delle chiavi integrata in ONTAP 9.5 e versioni precedenti (NVE)

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

A proposito di questa attività

È necessario eseguire `security key-manager setup` ogni volta che si aggiunge un nodo al cluster.

Se si dispone di una configurazione MetroCluster, consultare le seguenti linee guida:

- In ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale e. `security key-manager setup -sync-metrocluster-config yes` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.
- Prima di ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale, attendere circa 20 secondi, quindi eseguire `security key-manager setup` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente. Per `volume create`, non è necessario specificare `-encrypt true`. Per `volume move start`, non è necessario specificare `-encrypt-destination true`.

> Dopo un tentativo di passphrase non riuscito, riavviare nuovamente il nodo.

Prima di iniziare

- Se si utilizza NSE o NVE con un server KMIP (Key Management) esterno, è necessario eliminare il database del gestore delle chiavi esterno.

  "Passaggio alla gestione delle chiavi integrata dalla gestione delle chiavi esterna"

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare il Gestore chiavi integrato.

Fasi

1. Avviare la configurazione di Key Manager:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   > A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase del gestore delle chiavi dopo un riavvio. Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente.

   Nell'esempio seguente viene avviata l'impostazione del gestore delle chiavi sul cluster1 senza che sia necessario inserire la passphrase dopo ogni riavvio:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Invio `yes` quando viene richiesto di configurare la gestione delle chiavi integrata.
3. Al prompt della passphrase, immettere una passphrase compresa tra 32 e 256 caratteri oppure, per “cc-mode”, una passphrase compresa tra 64 e 256 caratteri.

> Se la passphrase “cc-mode” specificata è inferiore a 64 caratteri, si verifica un ritardo di cinque secondi prima che l’operazione di configurazione del gestore delle chiavi visualizzi nuovamente il prompt della passphrase.

4. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.
5. Verificare che le chiavi siano configurate per tutti i nodi:

   `security key-manager key show`

   Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

6. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

   `volume encryption conversion start`

   Onboard Key Manager deve essere completamente configurato prima di convertire i volumi. In un ambiente MetroCluster, il gestore delle chiavi integrato deve essere configurato su entrambi i siti.

Al termine

Copiare la passphrase in una posizione sicura all'esterno del sistema di storage per utilizzarla in futuro.

Ogni volta che si configura la passphrase di Onboard Key Manager, è necessario eseguire il backup manuale delle informazioni in una posizione sicura all'esterno del sistema di storage per l'utilizzo in caso di disastro. Vedere "Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate".

Abilitare la gestione delle chiavi integrata nei nodi appena aggiunti

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

> Per ONTAP 9.5 e versioni precedenti, è necessario eseguire `security key-manager setup` ogni volta che si aggiunge un nodo al cluster.
>
> Per ONTAP 9.6 e versioni successive, è necessario eseguire `security key-manager sync` ogni volta che si aggiunge un nodo al cluster.
>
> Se si aggiunge un nodo a un cluster che ha configurato la gestione delle chiavi integrate, eseguire questo comando per aggiornare le chiavi mancanti.

Se si dispone di una configurazione MetroCluster, consultare le seguenti linee guida:

- A partire da ONTAP 9.6, è necessario eseguire `security key-manager onboard enable` sul cluster locale, quindi eseguire `security key-manager onboard sync` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.
- In ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale e. `security key-manager setup -sync-metrocluster-config yes` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.
- Prima di ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale, attendere circa 20 secondi, quindi eseguire `security key-manager setup` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente. Per `volume create`, non è necessario specificare `-encrypt true`. Per `volume move start`, non è necessario specificare `-encrypt-destination true`.

> Dopo un tentativo di passphrase non riuscito, riavviare nuovamente il nodo.

Crittografare i dati del volume con NVE

Crittografare i dati del volume con la panoramica di NVE

A partire da ONTAP 9.7, la crittografia aggregata e del volume è attivata per impostazione predefinita quando si dispone della licenza VE e della gestione delle chiavi integrata o esterna. Per ONTAP 9.6 e versioni precedenti, è possibile attivare la crittografia su un nuovo volume o su un volume esistente. Prima di attivare la crittografia dei volumi, è necessario aver installato la licenza VE e attivato la gestione delle chiavi. NVE è conforme a FIPS-140-2 livello 1.

Abilitare la crittografia a livello aggregato con la licenza VE

A partire da ONTAP 9,7, gli aggregati e i volumi appena creati sono crittografati per impostazione predefinita, quando si dispone di "Licenza VE" e gestione della chiave integrata o esterna. A partire da ONTAP 9.6, è possibile utilizzare la crittografia a livello di aggregato per assegnare le chiavi all'aggregato contenente per i volumi da crittografare.

A proposito di questa attività

Se si intende eseguire la deduplica a livello di aggregato inline o in background, è necessario utilizzare la crittografia a livello di aggregato. La deduplica a livello di aggregato non è altrimenti supportata da NVE.

Un aggregato abilitato per la crittografia a livello di aggregato è denominato *aggregato NAE* (per NetApp aggregate Encryption). Tutti i volumi in un aggregato NAE devono essere crittografati con crittografia NAE o NVE. Con la crittografia a livello di aggregato, i volumi creati nell'aggregato vengono crittografati con la crittografia NAE per impostazione predefinita. È possibile eseguire l'override del valore predefinito per utilizzare la crittografia NVE.

I volumi di testo normale non sono supportati negli aggregati NAE.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fasi

1. Attivare o disattivare la crittografia a livello di aggregato:

Per…	Utilizzare questo comando…
Creare un aggregato NAE con ONTAP 9.7 o versione successiva	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
Crea un aggregato NAE con ONTAP 9.6	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Convertire un aggregato non NAE in un aggregato NAE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`

Convertire un aggregato NAE in un aggregato non NAE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

Per la sintassi completa dei comandi, vedere le pagine man.

Il seguente comando attiva la crittografia a livello di aggregato `aggr1`:

- ONTAP 9.7 o versione successiva:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 o versioni precedenti:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. Verificare che l'aggregato sia abilitato per la crittografia:

   `storage aggregate show -fields encrypt-with-aggr-key`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Il seguente comando verifica `aggr1` è abilitato per la crittografia:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

Al termine

Eseguire `volume create` per creare i volumi crittografati.

Se si utilizza un server KMIP per memorizzare le chiavi di crittografia di un nodo, ONTAP "invia automaticamente" una chiave di crittografia al server quando si crittografa un volume.

Attivare la crittografia su un nuovo volume

È possibile utilizzare `volume create` per attivare la crittografia su un nuovo volume.

A proposito di questa attività

È possibile crittografare i volumi utilizzando NetApp Volume Encryption (NVE) e, a partire da ONTAP 9.6, NetApp aggregate Encryption (NAE). Per ulteriori informazioni su NAE e NVE, fare riferimento a. panoramica

sulla crittografia dei volumi.

La procedura per attivare la crittografia su un nuovo volume in ONTAP varia in base alla versione di ONTAP in uso e alla configurazione specifica:

- A partire da ONTAP 9.4, se si attiva `cc-mode` Quando si configura Onboard Key Manager, i volumi creati con `volume create` i comandi vengono crittografati automaticamente, indipendentemente dal fatto che l'utente lo specifichi o meno `-encrypt true`.
- In ONTAP 9.6 e versioni precedenti, è necessario utilizzare `-encrypt true` con `volume create` comandi per attivare la crittografia (a condizione che non sia stata attivata) `cc-mode`).
- Se si desidera creare un volume NAE in ONTAP 9.6, è necessario attivare NAE a livello di aggregato. Fare riferimento a. Abilitare la crittografia a livello di aggregato con la licenza VE per ulteriori dettagli su questa attività.
- A partire da ONTAP 9,7, i volumi appena creati vengono crittografati per impostazione predefinita quando si dispone di "Licenza VE" e gestione della chiave integrata o esterna. Per impostazione predefinita, i nuovi volumi creati in un aggregato NAE saranno di tipo NAE anziché NVE.
  - In ONTAP 9.7 e versioni successive, se si aggiunge `-encrypt true` al `volume create` Comando per creare un volume in un aggregato NAE, il volume avrà la crittografia NVE invece di NAE. Tutti i volumi in un aggregato NAE devono essere crittografati con NVE o NAE.

> I volumi non in testo normale non sono supportati negli aggregati NAE.

Fasi

1. Creare un nuovo volume e specificare se la crittografia è attivata sul volume. Se il nuovo volume si trova in un aggregato NAE, per impostazione predefinita il volume sarà un volume NAE:

Per creare…	Utilizzare questo comando…
Un volume NAE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
Un volume NVE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` + In ONTAP 9.6 e versioni precedenti, dove non è supportato il servizio NAE, `-encrypt true` Specifica che il volume deve essere crittografato con NVE. In ONTAP 9.7 e versioni successive, dove i volumi vengono creati in aggregati NAE, `-encrypt true` Esegue l'override del tipo di crittografia predefinito di NAE per creare un volume NVE.
Un volume di testo normale	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

   Per la sintassi completa dei comandi, fare riferimento alla pagina di riferimento dei comandi per `volume create`.

2. Verificare che i volumi siano abilitati per la crittografia:

```
volume show -is-encrypted true
```

Per la sintassi completa dei comandi, vedere "riferimento al comando".

Risultato

Se si utilizza un server KMIP per memorizzare le chiavi di crittografia di un nodo, ONTAP "invia" automaticamente una chiave di crittografia al server quando si crittografa un volume.

=
:allow-uri-read:

Attivare la crittografia su un volume esistente

È possibile utilizzare il `volume move start` o il `volume encryption conversion start` per abilitare la crittografia su un volume esistente.

A proposito di questa attività

- A partire da ONTAP 9.3, è possibile utilizzare `volume encryption conversion start` comando per abilitare la crittografia di un volume esistente "sul posto", senza dover spostare il volume in una posizione diversa. In alternativa, è possibile utilizzare `volume move start` comando.
- Per ONTAP 9,2 e versioni precedenti, è possibile utilizzare solo `volume move start` per attivare la crittografia spostando un volume esistente.

Attivare la crittografia su un volume esistente con il comando di avvio della conversione della crittografia del volume

A partire da ONTAP 9.3, è possibile utilizzare `volume encryption conversion start` comando per abilitare la crittografia di un volume esistente "sul posto", senza dover spostare il volume in una posizione diversa.

Dopo aver avviato un'operazione di conversione, è necessario completarla. Se si verificano problemi di prestazioni durante l'operazione, è possibile eseguire `volume encryption conversion pause` per sospendere l'operazione e il `volume encryption conversion resume` per riprendere l'operazione.

> Non è possibile utilizzare `volume encryption conversion start` Per convertire un volume SnapLock.

Fasi

1. Abilitare la crittografia su un volume esistente:

   ```
   volume encryption conversion start -vserver SVM_name -volume volume_name
   ```

   Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

   Il seguente comando consente la crittografia sul volume esistente `vol1`:

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   Il sistema crea una chiave di crittografia per il volume. I dati del volume vengono crittografati.

2. Verificare lo stato dell'operazione di conversione:

   `volume encryption conversion show`

   Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

   Il seguente comando visualizza lo stato dell'operazione di conversione:

```
cluster1::> volume encryption conversion show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   ---------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. Una volta completata l'operazione di conversione, verificare che il volume sia abilitato per la crittografia:

   `volume show -is-encrypted true`

   Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

   Il seguente comando visualizza i volumi crittografati su `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Risultato

Se si utilizza un server KMIP per memorizzare le chiavi di crittografia di un nodo, ONTAP "invia automaticamente" una chiave di crittografia al server quando si crittografa un volume.

Attivare la crittografia su un volume esistente con il comando di avvio spostamento volume

È possibile utilizzare `volume move start` per attivare la crittografia spostando un volume esistente. È necessario utilizzare `volume move start` In ONTAP 9.2 e versioni precedenti. È possibile utilizzare lo stesso aggregato o un aggregato diverso.

A proposito di questa attività

- A partire da ONTAP 9.8, è possibile utilizzare `volume move start` Per attivare la crittografia su un volume SnapLock o FlexGroup.
- A partire da ONTAP 9.4, se si attiva "cc-mode" quando si imposta il Gestore chiavi integrato, i volumi creati con `volume move start` i comandi vengono crittografati automaticamente. Non è necessario specificare `-encrypt-destination true`.
- A partire da ONTAP 9.6, è possibile utilizzare la crittografia a livello di aggregato per assegnare le chiavi all'aggregato contenente per i volumi da spostare. Un volume crittografato con una chiave univoca è chiamato *volume NVE* (ovvero utilizza la crittografia del volume NetApp). Un volume crittografato con una

chiave a livello di aggregato viene chiamato *volume NAE* (per NetApp aggregate Encryption). I volumi non in testo normale non sono supportati negli aggregati NAE.

- A partire da ONTAP 9.14.1, puoi crittografare un volume root di una SVM con NVE. Per ulteriori informazioni, vedere Configurare la crittografia dei volumi NetApp su un volume root della SVM.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o un amministratore SVM al quale l'amministratore del cluster ha delegato l'autorità.

"Delega dell'autorizzazione all'esecuzione del comando di spostamento del volume"

Fasi

1. Spostare un volume esistente e specificare se la crittografia è attivata sul volume:

Per convertire…	Utilizzare questo comando…
Un volume non crittografato su un volume NVE	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true`
Un volume NVE o plaintext su un volume NAE (supponendo che la crittografia a livello di aggregato sia attivata sulla destinazione)	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key true`
Un volume NAE su un volume NVE	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key false`
Un volume NAE su un volume non crittografato	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false -encrypt-with-aggr-key false`
Un volume NVE su un volume non crittografato	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

Il seguente comando converte un volume non crittografato denominato `vol1` Su un volume NVE:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Supponendo che la crittografia a livello di aggregato sia attivata sulla destinazione, il seguente comando converte un volume NVE o non crittografato denominato `vol1` Su un volume NAE:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

Il seguente comando converte un volume NAE denominato `vol2` Su un volume NVE:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

Il seguente comando converte un volume NAE denominato `vol2` su un volume non crittografato:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

Il seguente comando converte un volume NVE denominato `vol2` su un volume non crittografato:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. Visualizzare il tipo di crittografia dei volumi del cluster:

   `volume show -fields encryption-type none|volume|aggregate`

   Il `encryption-type` Field è disponibile in ONTAP 9.6 e versioni successive.

   Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

   Il seguente comando visualizza il tipo di crittografia dei volumi in `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. Verificare che i volumi siano abilitati per la crittografia:

   `volume show -is-encrypted true`

   Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

   Il seguente comando visualizza i volumi crittografati su `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Risultato

Se si utilizza un server KMIP per memorizzare le chiavi di crittografia di un nodo, ONTAP invia automaticamente una chiave di crittografia al server quando si crittografa un volume.

Configurare la crittografia dei volumi NetApp su un volume root della SVM

A partire da ONTAP 9.14.1, puoi abilitare NetApp Volume Encryption (NVE) su un volume root di una Storage VM (SVM). Con NVE, il volume root è crittografato con una chiave univoca, abilitando una maggiore sicurezza sulla SVM.

A proposito di questa attività

NVE su un volume root di SVM può essere abilitato solo dopo che è stata creata la SVM.

Prima di iniziare

- Il volume root della SVM non deve trovarsi in un aggregato crittografato con crittografia degli aggregati NetApp (NAE).
- È necessario aver abilitato la crittografia con Onboard Key Manager o con un gestore di chiavi esterno.
- È necessario eseguire ONTAP 9.14.1 o versione successiva.
- Per migrare una SVM contenente un volume root crittografato con NVE, al termine della migrazione è necessario convertire il volume root della SVM in un volume di testo normale, quindi crittografare di nuovo il volume root della SVM.
  - Se l'aggregato di destinazione della migrazione SVM utilizza NAE, il volume root eredita NAE per impostazione predefinita.
- Se la SVM si trova in una relazione di disaster recovery della SVM:
  - Le impostazioni di crittografia su una SVM con mirroring non vengono copiate nella destinazione. Se abiliti NVE sull'origine o sulla destinazione, devi abilitare NVE separatamente sul volume root della SVM con mirroring.
  - Se tutti gli aggregati nel cluster di destinazione utilizzano NAE, il volume root della SVM utilizzerà NAE.

Fasi

Puoi abilitare NVE su un volume root di SVM con l'interfaccia a riga di comando di ONTAP o System Manager.

CLI

È possibile abilitare NVE sul volume root della SVM in-place o spostando il volume tra aggregati.

Crittografare il volume root in uso

1. Convertire il volume root in un volume crittografato:

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. Conferma crittografia riuscita. Il `volume show -encryption-type volume` Visualizza un elenco di tutti i volumi che utilizzano NVE.

Crittografa il volume root della SVM spostandolo

1. Avvio dello spostamento di un volume:

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

   Per ulteriori informazioni su `volume move`, vedere Spostare un volume.

2. Confermare `volume move` operazione riuscita con il `volume move show` comando. Il `volume show -encryption-type volume` Visualizza un elenco di tutti i volumi che utilizzano NVE.

System Manager

1. Passare a **archiviazione** > **volumi**.
2. Selezionare, accanto al nome del volume root della SVM che si desidera crittografare ⋮ Poi **Modifica**.
3. Sotto l'intestazione **archiviazione e ottimizzazione**, selezionare **Abilita crittografia**.
4. Selezionare **Salva**.

Abilitare la crittografia del volume root del nodo

A partire da ONTAP 9.8, è possibile utilizzare la crittografia dei volumi NetApp per proteggere il volume root del nodo.

> **A proposito di questa attività**
>
> Questa procedura si applica al volume root del nodo. Non si applica ai volumi root SVM. I volumi root delle SVM possono essere protetti tramite crittografia a livello di aggregato e A partire da ONTAP 9.14.1, NVE.

Una volta avviata, la crittografia del volume root deve essere completata. Non è possibile sospendere l'operazione. Una volta completata la crittografia, non è possibile assegnare una nuova chiave al volume root e non è possibile eseguire un'operazione di eliminazione sicura.

Prima di iniziare

- Il sistema deve utilizzare una configurazione ha.
- Il volume root del nodo deve essere già creato.
- Il sistema deve disporre di un gestore delle chiavi integrato o di un server di gestione delle chiavi esterno che utilizzi il protocollo KMIP (Key Management Interoperability Protocol).

Fasi

1. Crittografare il volume root:

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. Verificare lo stato dell'operazione di conversione:

   ```
   volume encryption conversion show
   ```

3. Una volta completata l'operazione di conversione, verificare che il volume sia crittografato:

   ```
   volume show -fields
   ```

   Di seguito viene riportato un esempio di output per un volume crittografato.

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```

Configurare la crittografia basata su hardware NetApp

Configurazione della panoramica della crittografia basata su hardware NetApp

La crittografia basata su hardware di NetApp supporta la crittografia completa dei dischi (FDE) dei dati così come vengono scritti. I dati non possono essere letti senza una chiave di crittografia memorizzata nel firmware. La chiave di crittografia, a sua volta, è accessibile solo a un nodo autenticato.

Comprendere la crittografia basata su hardware NetApp

Un nodo esegue l'autenticazione su un'unità con crittografia automatica utilizzando una chiave di autenticazione recuperata da un server di gestione delle chiavi esterno o da Onboard Key Manager:

- Il server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol). Si consiglia di configurare i server di gestione delle chiavi esterni su un sistema storage diverso dai dati.
- Onboard Key Manager è uno strumento integrato che fornisce chiavi di autenticazione ai nodi dello stesso sistema storage dei dati.

È possibile utilizzare NetApp Volume Encryption con crittografia basata su hardware per "eseguire la doppia crittografia `d`" dei dati su dischi con crittografia automatica.

Quando i dischi con crittografia automatica sono abilitati, anche il core dump è crittografato.

> Se una coppia ha utilizza dischi SAS o NVMe con crittografia (SED, NSE, FIPS), seguire le istruzioni riportate nell'argomento Ripristino di un'unità FIPS o SED in modalità non protetta Per tutti i dischi all'interno della coppia ha prima dell'inizializzazione del sistema (opzioni di avvio 4 o 9). Il mancato rispetto di questa procedura potrebbe causare la perdita di dati in futuro se i dischi vengono riutilizzati.

Tipi di dischi con crittografia automatica supportati

Sono supportati due tipi di dischi con crittografia automatica:

- I dischi SAS o NVMe con crittografia automatica certificati FIPS sono supportati su tutti i sistemi FAS e AFF. Questi dischi, denominati *dischi FIPS,* sono conformi ai requisiti della pubblicazione Federal Information Processing Standard 140-2, livello 2. Le funzionalità certificate consentono di proteggere oltre alla crittografia, ad esempio prevenendo attacchi di tipo Denial-of-service sul disco. I dischi FIPS non possono essere combinati con altri tipi di dischi sullo stesso nodo o coppia ha.
- A partire da ONTAP 9.6, i dischi NVMe con crittografia automatica che non hanno superato i test FIPS sono supportati sui sistemi AFF A800, A320 e successivi. Questi dischi, denominati *SED*, offrono le stesse funzionalità di crittografia dei dischi FIPS, ma possono essere combinati con dischi non crittografanti sullo stesso nodo o coppia ha.
- Tutti i dischi convalidati FIPS utilizzano un modulo di crittografia del firmware che è stato eseguito attraverso la convalida FIPS. Il modulo crittografico del disco FIPS non utilizza chiavi generate al di fuori del disco (la passphrase di autenticazione immessa nel disco viene utilizzata dal modulo crittografico del firmware del disco per ottenere una chiave di crittografia).

> Le unità non crittografate sono unità che non sono unità SED o FIPS.

> Se stai utilizzando NSE su un sistema con un modulo Flash cache, dovresti abilitare anche NVE o NAE. NSe non crittografa i dati che risiedono nel modulo Flash cache.

Quando utilizzare la gestione esterna delle chiavi

Sebbene sia meno costoso e generalmente più conveniente utilizzare il gestore delle chiavi integrato, è consigliabile utilizzare la gestione esterna delle chiavi se si verifica una delle seguenti condizioni:

- La policy aziendale richiede una soluzione di gestione delle chiavi che utilizzi un modulo crittografico FIPS 140-2 livello 2 (o superiore).
- Hai bisogno di una soluzione multi-cluster, con gestione centralizzata delle chiavi di crittografia.
- La tua azienda richiede una maggiore sicurezza nell'archiviazione delle chiavi di autenticazione su un sistema o in una posizione diversa dai dati.

Dettagli del supporto

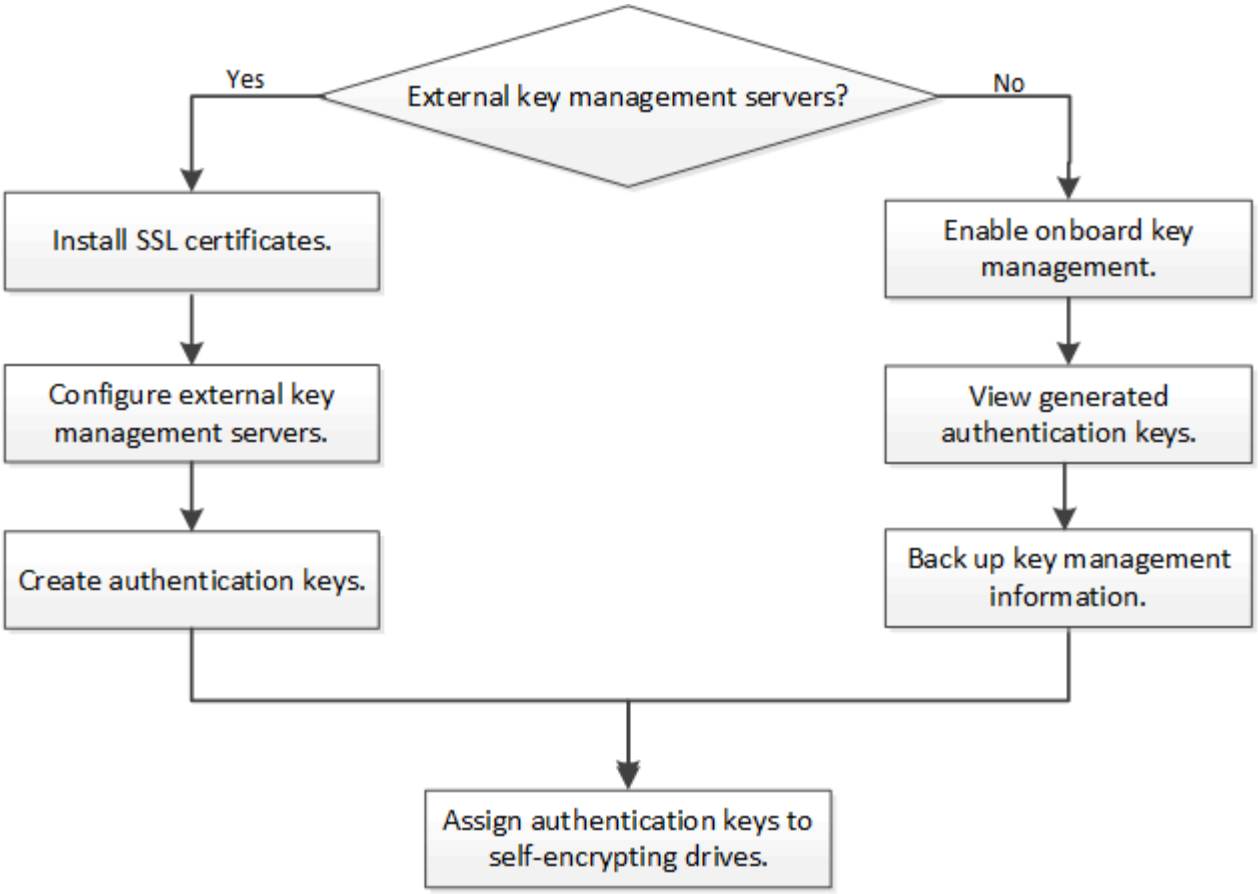
La seguente tabella mostra importanti dettagli sul supporto della crittografia hardware. Consulta la matrice di interoperabilità per le informazioni più recenti su server KMIP, sistemi storage e shelf di dischi supportati.

Risorsa o funzione	Dettagli del supporto

Set di dischi non omogenei	• I dischi FIPS non possono essere combinati con altri tipi di dischi sullo stesso nodo o coppia ha. Le coppie ha conformi possono coesistere con coppie ha non conformi nello stesso cluster. • È possibile combinare i dischi con dischi non crittografanti sullo stesso nodo o coppia ha.
Tipo di disco	• I dischi FIPS possono essere SAS o NVMe. • I dischi Sed devono essere NVMe.
Interfacce di rete da 10 GB	A partire da ONTAP 9.3, le configurazioni di gestione delle chiavi KMIP supportano interfacce di rete da 10 GB per le comunicazioni con server di gestione delle chiavi esterni.
Porte per la comunicazione con il server di gestione delle chiavi	A partire da ONTAP 9.3, è possibile utilizzare qualsiasi porta del controller di storage per la comunicazione con il server di gestione delle chiavi. In caso contrario, utilizzare la porta e0M per la comunicazione con i server di gestione delle chiavi. A seconda del modello di controller di storage, alcune interfacce di rete potrebbero non essere disponibili durante il processo di avvio per la comunicazione con i server di gestione delle chiavi.
MetroCluster (MCC)	• I dischi NVMe supportano MCC. • I dischi SAS non supportano MCC.

Workflow di crittografia basato su hardware

È necessario configurare i servizi di gestione delle chiavi prima che il cluster possa autenticarsi sull'unità con crittografia automatica. È possibile utilizzare un server di gestione delle chiavi esterno o un gestore delle chiavi integrato.



Informazioni correlate

- "NetApp Hardware Universe"
- "NetApp Volume Encryption e NetApp aggregate Encryption"

Configurare la gestione esterna delle chiavi

Configurare una panoramica sulla gestione esterna delle chiavi

È possibile utilizzare uno o più server di gestione delle chiavi esterni per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. Un server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol).

Per ONTAP 9.1 e versioni precedenti, è necessario assegnare le LIF di gestione dei nodi alle porte configurate con il ruolo di gestione dei nodi prima di poter utilizzare il gestore delle chiavi esterno.

La crittografia dei volumi NetApp (NVE) può essere implementata con Onboard Key Manager in ONTAP 9.1 e versioni successive. In ONTAP 9.3 e versioni successive, NVE può essere implementato con gestione delle chiavi esterna (KMIP) e Gestione delle chiavi integrata. A partire da ONTAP 9.11.1, è possibile configurare più Key Manager esterni in un cluster. Vedere Configurare i server delle chiavi in cluster.

Raccogliere le informazioni di rete in ONTAP 9.2 e versioni precedenti

Se si utilizza ONTAP 9.2 o versioni precedenti, compilare il foglio di lavoro per la configurazione di rete prima di attivare la gestione esterna delle chiavi.

A partire da ONTAP 9.3, il sistema rileva automaticamente tutte le informazioni di rete necessarie.

Elemento	Note	Valore
Nome dell'interfaccia di rete per la gestione delle chiavi		
Indirizzo IP dell'interfaccia di rete per la gestione delle chiavi	Indirizzo IP della LIF di gestione dei nodi, in formato IPv4 o IPv6	
Gestione delle chiavi interfaccia di rete IPv6 lunghezza prefisso di rete	Se si utilizza IPv6, la lunghezza del prefisso di rete IPv6	
Subnet mask dell'interfaccia di rete per la gestione delle chiavi		
Gestione delle chiavi Indirizzo IP del gateway dell'interfaccia di rete		
Indirizzo IPv6 per l'interfaccia di rete del cluster	Obbligatorio solo se si utilizza IPv6 per l'interfaccia di rete per la gestione delle chiavi	
Numero di porta per ciascun server KMIP	Opzionale. Il numero di porta deve essere lo stesso per tutti i server KMIP. Se non si specifica un numero di porta, per impostazione predefinita viene impostata la porta 5696, che corrisponde alla porta assegnata dall'autorità IANA (Internet Assigned Numbers Authority) per KMIP.	
Nome tag chiave	Opzionale. Il nome del tag della chiave viene utilizzato per identificare tutte le chiavi appartenenti a un nodo. Il nome predefinito del tag della chiave è il nome del nodo.	

Informazioni correlate

"Report tecnico di NetApp 3954: Requisiti e procedure di preinstallazione di NetApp Storage Encryption per IBM Tivoli Lifetime Key Manager"

"Report tecnico di NetApp 4074: Requisiti e procedure di preinstallazione di NetApp Storage Encryption per SafeNet KeySecure"

Installare i certificati SSL sul cluster

Il cluster e il server KMIP utilizzano i certificati SSL KMIP per verificare l'identità reciproca e stabilire una connessione SSL. Prima di configurare la connessione SSL con il server

KMIP, è necessario installare i certificati SSL del client KMIP per il cluster e il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.

A proposito di questa attività

In una coppia ha, entrambi i nodi devono utilizzare gli stessi certificati SSL KMIP pubblici e privati. Se si collegano più coppie ha allo stesso server KMIP, tutti i nodi delle coppie ha devono utilizzare gli stessi certificati SSL KMIP pubblici e privati.

Prima di iniziare

- L'ora deve essere sincronizzata sul server che crea i certificati, sul server KMIP e sul cluster.
- È necessario avere ottenuto il certificato del client KMIP SSL pubblico per il cluster.
- È necessario aver ottenuto la chiave privata associata al certificato del client SSL KMIP per il cluster.
- Il certificato del client SSL KMIP non deve essere protetto da password.
- È necessario aver ottenuto il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.
- In un ambiente MetroCluster, è necessario installare gli stessi certificati SSL KMIP su entrambi i cluster.

> È possibile installare i certificati client e server sul server KMIP prima o dopo l'installazione dei certificati sul cluster.

Fasi

1. Installare i certificati del client KMIP SSL per il cluster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   Viene richiesto di immettere i certificati SSL KMIP pubblici e privati.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Installare il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP:

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Gestione esterna delle chiavi in ONTAP 9.6 e versioni successive (basato su hardware)

È possibile utilizzare uno o più server KMIP per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È possibile collegare fino a quattro server KMIP a un nodo. Si consiglia di utilizzare almeno due server per la ridondanza e il disaster recovery.

A partire da ONTAP 9.11.1, è possibile aggiungere fino a 3 server di chiavi secondari per ogni server di chiavi primario per creare un server di chiavi in cluster. Per ulteriori informazioni, vedere Configurare i server di chiavi esterne in cluster.

Prima di iniziare

- I certificati del server e del client SSL KMIP devono essere stati installati.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

- È necessario configurare l'ambiente MetroCluster prima di configurare un gestore di chiavi esterno.
- In un ambiente MetroCluster, è necessario installare il certificato SSL KMIP su entrambi i cluster.

Fasi

1. Configurare la connettività del gestore delle chiavi per il cluster:

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   > - Il `security key-manager external enable` il comando sostituisce `security key-manager setup` comando. È possibile eseguire `security key-manager external modify` comando per modificare la configurazione di gestione delle chiavi esterne. Per la sintassi completa dei comandi, vedere le pagine man.
   > - In un ambiente MetroCluster, se si sta configurando la gestione esterna delle chiavi per la SVM amministrativa, è necessario ripetere `security key-manager external enable` sul cluster partner.

   Il seguente comando abilita la gestione esterna delle chiavi per `cluster1` con tre key server esterni. Il primo server chiavi viene specificato utilizzando il nome host e la porta, il secondo viene specificato utilizzando un indirizzo IP e la porta predefinita, mentre il terzo viene specificato utilizzando un indirizzo IPv6 e una porta:

   ```
   clusterl::> security key-manager external enable -key-servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. Verificare che tutti i server KMIP configurati siano connessi:

   ```
   security key-manager external show-status -node node_name -vserver SVM -key
   -server host_name|IP_address:port -key-server-status available|not-
   responding|unknown
   ```

   > Il `security key-manager external show-status` il comando sostituisce `security key-manager show -status` comando. Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ----------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

Abilitare la gestione esterna delle chiavi in ONTAP 9.5 e versioni precedenti

È possibile utilizzare uno o più server KMIP per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È possibile collegare fino a quattro server KMIP a un nodo. Si consiglia di utilizzare almeno due server per la ridondanza e il disaster recovery.

A proposito di questa attività

ONTAP configura la connettività del server KMIP per tutti i nodi del cluster.

Prima di iniziare

- I certificati del server e del client SSL KMIP devono essere stati installati.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare un gestore di chiavi esterno.
- In un ambiente MetroCluster, è necessario installare il certificato SSL KMIP su entrambi i cluster.

Fasi

1. Configurare la connettività del gestore delle chiavi per i nodi del cluster:

   ```
   security key-manager setup
   ```

   Viene avviata la configurazione di Key Manager.

   > In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

2. Immettere la risposta appropriata a ogni richiesta.
3. Aggiunta di un server KMIP:

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

```
clusterl::> security key-manager add -address 20.1.1.1
```

In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

4. Aggiungere un server KMIP aggiuntivo per la ridondanza:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

5. Verificare che tutti i server KMIP configurati siano connessi:

   `security key-manager show -status`

   Per la sintassi completa dei comandi, vedere la pagina man.

   ```
   cluster1::> security key-manager show -status

   Node            Port      Registered Key Manager  Status
   --------------  ----      ----------------------  ---------------
   cluster1-01     5696      20.1.1.1                available
   cluster1-01     5696      20.1.1.2                available
   cluster1-02     5696      20.1.1.1                available
   cluster1-02     5696      20.1.1.2                available
   ```

6. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

   `volume encryption conversion start`

   Prima di convertire i volumi, è necessario configurare completamente un gestore di chiavi esterno. In un ambiente MetroCluster, è necessario configurare un gestore di chiavi esterno su entrambi i siti.

Configurare i server di chiavi esterne in cluster

A partire da ONTAP 9.11.1, è possibile configurare la connettività ai server di gestione delle chiavi esterni in cluster su una SVM. Con i key server in cluster, è possibile designare i key server primari e secondari su una SVM. Durante la registrazione delle chiavi, ONTAP tenta innanzitutto di accedere a un server principale prima di tentare di accedere in sequenza ai server secondari fino al completamento dell'operazione, evitando la duplicazione delle chiavi.

I Key server esterni possono essere utilizzati per le chiavi NSE, NVE, NAE e SED. Una SVM può supportare fino a quattro server KMIP esterni primari. Ciascun server primario può supportare fino a tre server secondari

per le chiavi.

Prima di iniziare

- "La gestione delle chiavi di KMIP deve essere abilitata per la SVM".
- Questo processo supporta solo i server chiave che utilizzano KMIP. Per un elenco dei server delle chiavi supportati, consultare "Tool di matrice di interoperabilità NetApp".
- Tutti i nodi del cluster devono eseguire ONTAP 9.11.1 o versione successiva.
- L'ordine dei server elenca gli argomenti in `-secondary-key-servers` Il parametro riflette l'ordine di accesso dei server KMIP (gestione delle chiavi esterne).

Creare un server di chiavi in cluster

La procedura di configurazione dipende dal fatto che sia stato configurato o meno un server di chiavi primario.

Aggiunta di server di chiavi primari e secondari a una SVM

1. Verificare che non sia stata attivata alcuna gestione delle chiavi per il cluster:
   `security key-manager external show -vserver` *`svm_name`*
   Se SVM ha già attivato un massimo di quattro server principali, è necessario rimuovere uno dei server principali esistenti prima di aggiungerne uno nuovo.
2. Attivare il gestore delle chiavi primario:
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. Modificare il server delle chiavi primario per aggiungere i server delle chiavi secondari. Il `-secondary-key-servers` parameter accetta un elenco separato da virgole di un massimo di tre server chiave.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

Aggiungere i server di chiavi secondari a un server di chiavi primario esistente

1. Modificare il server delle chiavi primario per aggiungere i server delle chiavi secondari. Il `-secondary-key-servers` parameter accetta un elenco separato da virgole di un massimo di tre server chiave.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*
   Per ulteriori informazioni sui server di chiavi secondari, vedere [mod-secondary].

Modificare i server delle chiavi in cluster

È possibile modificare i cluster di Key Server esterni modificando lo stato (primario o secondario) di determinati Key Server, aggiungendo e rimuovendo i Key Server secondari o modificando l'ordine di accesso dei Key Server secondari.

Convertire i server chiavi primari e secondari

Per convertire un server di chiavi primario in un server di chiavi secondario, è necessario prima rimuoverlo dalla SVM con `security key-manager external remove-servers` comando.

Per convertire un server chiavi secondario in un server chiavi primario, è necessario prima rimuovere il server chiavi secondario dal server chiavi primario esistente. Vedere [mod-secondary]. Se si converte un server chiavi secondario in un server primario durante la rimozione di una chiave esistente, il tentativo di aggiungere un nuovo server prima di completare la rimozione e la conversione può comportare la duplicazione delle chiavi.

Modificare i server chiavi secondari

I server di chiavi secondari vengono gestiti con `-secondary-key-servers` del parametro `security key-manager external modify-server` comando. Il `-secondary-key-servers` parameter accetta un elenco separato da virgole. L'ordine specificato dei server di chiavi secondari nell'elenco determina la sequenza di accesso per i server di chiavi secondari. L'ordine di accesso può essere modificato eseguendo il comando `security key-manager external modify-server` con i server di chiavi secondari inseriti in una sequenza diversa.

Per rimuovere un server di chiavi secondario, la `-secondary-key-servers` gli argomenti devono includere i server chiave che si desidera conservare mentre si omette quello da rimuovere. Per rimuovere tutti i server di chiavi secondari, utilizzare l'argomento `-`, non significa nessuno.

Per ulteriori informazioni, fare riferimento a. `security key-manager external` nella "Riferimento al comando ONTAP".

Creare chiavi di autenticazione in ONTAP 9.6 e versioni successive

È possibile utilizzare `security key-manager key create` Per creare le chiavi di autenticazione per un nodo e memorizzarle nei server KMIP configurati.

A proposito di questa attività

Se la configurazione della protezione richiede l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2, è necessario creare una chiave separata per ciascuna di esse. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

ONTAP crea chiavi di autenticazione per tutti i nodi del cluster.

- Questo comando non è supportato quando Onboard Key Manager è attivato. Tuttavia, quando Onboard Key Manager è attivato, vengono create automaticamente due chiavi di autenticazione. I tasti possono essere visualizzati con il seguente comando:

  ```
  security key-manager key query -key-type NSE-AK
  ```

- Viene visualizzato un avviso se i server di gestione delle chiavi configurati memorizzano già più di 128 chiavi di autenticazione.
- È possibile utilizzare `security key-manager key delete` per eliminare le chiavi inutilizzate. Il `security key-manager key delete` Il comando non riesce se la chiave è attualmente in uso da ONTAP. Per utilizzare questo comando, è necessario disporre di privilegi superiori a "admin".

> In un ambiente MetroCluster, prima di eliminare una chiave, è necessario assicurarsi che la chiave non sia in uso nel cluster partner. È possibile utilizzare i seguenti comandi sul cluster partner per verificare che la chiave non sia in uso:
>
> - `storage encryption disk show -data-key-id` *`key-id`*
> - `storage encryption disk show -fips-key-id` *`key-id`*

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fasi

1. Creare le chiavi di autenticazione per i nodi del cluster:

   ```
   security key-manager key create -key-tag passphrase_label -prompt-for-key
   true|false
   ```

   > Impostazione `prompt-for-key=true` fa in modo che il sistema richieda all'amministratore del cluster la passphrase da utilizzare per l'autenticazione dei dischi crittografati. In caso contrario, il sistema genera automaticamente una passphrase da 32 byte. Il `security key-manager key create` il comando sostituisce `security key-manager create-key` comando. Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente vengono create le chiavi di autenticazione per `cluster1`, che genera automaticamente una passphrase da 32 byte:

   ```
   cluster1::> security key-manager key create
   Key ID:
   00000000000000000200000000000001006268333f870860128fbe17d393e5083b00000000
   00000000
   ```

2. Verificare che le chiavi di autenticazione siano state create:

   ```
   security key-manager key query -node node
   ```

   > Il `security key-manager key query` il comando sostituisce `security key-manager query key` comando. Per la sintassi completa dei comandi, vedere la pagina man. L'ID della chiave visualizzato nell'output è un identificatore utilizzato per fare riferimento alla chiave di autenticazione. Non si tratta della chiave di autenticazione effettiva o della chiave di crittografia dei dati.

   Nell'esempio seguente viene verificata la creazione di chiavi di autenticazione per `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Creare chiavi di autenticazione in ONTAP 9.5 e versioni precedenti

È possibile utilizzare `security key-manager create-key` Per creare le chiavi di autenticazione per un nodo e memorizzarle nei server KMIP configurati.

A proposito di questa attività

Se la configurazione della protezione richiede l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2, è necessario creare una chiave separata per ciascuna di esse. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

ONTAP crea chiavi di autenticazione per tutti i nodi del cluster.

- Questo comando non è supportato quando è attivata la gestione delle chiavi integrate.
- Viene visualizzato un avviso se i server di gestione delle chiavi configurati memorizzano già più di 128 chiavi di autenticazione.

È possibile utilizzare il software del server di gestione delle chiavi per eliminare le chiavi inutilizzate, quindi eseguire nuovamente il comando.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fasi

1. Creare le chiavi di autenticazione per i nodi del cluster:

   `security key-manager create-key`

   Per la sintassi completa dei comandi, vedere la pagina man del comando.

   > L'ID della chiave visualizzato nell'output è un identificatore utilizzato per fare riferimento alla chiave di autenticazione. Non si tratta della chiave di autenticazione effettiva o della chiave di crittografia dei dati.

   Nell'esempio seguente vengono create le chiavi di autenticazione per `cluster1`:

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. Verificare che le chiavi di autenticazione siano state create:

   `security key-manager query`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene verificata la creazione di chiavi di autenticazione per `cluster1`:

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

Assegnazione di una chiave di autenticazione dei dati a un disco FIPS o SED (gestione esterna delle chiavi)

È possibile utilizzare `storage encryption disk modify` Comando per assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED. I nodi del cluster utilizzano questa chiave per bloccare o sbloccare i dati crittografati sul disco.

A proposito di questa attività

Un'unità con crittografia automatica è protetta da accessi non autorizzati solo se l'ID della chiave di autenticazione è impostato su un valore non predefinito. L'ID sicuro del produttore (MSID), con ID chiave 0x0, è il valore predefinito standard per i dischi SAS. Per i dischi NVMe, il valore predefinito standard è una chiave nulla, rappresentata come ID chiave vuoto. Quando si assegna l'ID della chiave a un'unità con crittografia automatica, il sistema modifica l'ID della chiave di autenticazione in un valore non predefinito.

Questa procedura non comporta interruzioni.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fasi

1. Assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED:

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

Per la sintassi completa dei comandi, vedere la pagina man del comando.

> È possibile utilizzare `security key-manager query -key-type NSE-AK` Per visualizzare gli ID chiave.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. Verificare che le chiavi di autenticazione siano state assegnate:

   `storage encryption disk show`

   Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
-------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
[...]
```

Configurare la gestione delle chiavi integrata

Attiva la gestione delle chiavi integrata in ONTAP 9.6 e versioni successive

È possibile utilizzare Onboard Key Manager per autenticare i nodi del cluster su un disco FIPS o SED. Onboard Key Manager è uno strumento integrato che fornisce chiavi di autenticazione ai nodi dello stesso sistema storage dei dati. Onboard Key Manager è conforme a FIPS-140-2 livello 1.

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

A proposito di questa attività

È necessario eseguire `security key-manager onboard enable` ogni volta che si aggiunge un nodo al cluster. Nelle configurazioni MetroCluster, è necessario eseguire `security key-manager onboard enable` sul cluster locale, quindi eseguire `security key-manager onboard sync` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. Ad eccezione di MetroCluster, è possibile utilizzare `cc-mode-enabled=yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Quando Onboard Key Manager è attivato in modalità Common Criteria (Criteri comuni) (`cc-mode-enabled=yes`), il comportamento del sistema viene modificato nei seguenti modi:

- Il sistema monitora i tentativi consecutivi di passphrase del cluster non riusciti quando si opera in modalità Common Criteria.

  Se NetApp Storage Encryption (NSE) è attivato e non si riesce a inserire la passphrase del cluster corretta all'avvio, il sistema non può autenticare i propri dischi e si riavvia automaticamente. Per risolvere il problema, al prompt di boot occorre inserire la passphrase del cluster corretta. Una volta avviato, il sistema consente fino a 5 tentativi consecutivi di inserire correttamente la passphrase del cluster in un periodo di 24 ore per qualsiasi comando che richieda la passphrase del cluster come parametro. Se il limite viene raggiunto (ad esempio, non è stato possibile inserire correttamente la passphrase del cluster 5 volte di seguito), è necessario attendere che il periodo di timeout di 24 ore sia trascorso oppure riavviare il nodo per ripristinare il limite.

- Gli aggiornamenti delle immagini di sistema utilizzano il certificato di firma del codice NetApp RSA-3072 insieme ai digest con firma del codice SHA-384 per controllare l'integrità dell'immagine invece del certificato di firma del codice NetApp RSA-2048 e dei digest con firma del codice SHA-256.

  Il comando upgrade verifica che il contenuto dell'immagine non sia stato alterato o corrotto controllando varie firme digitali. Se la convalida ha esito positivo, il processo di aggiornamento dell'immagine passa alla fase successiva; in caso contrario, l'aggiornamento dell'immagine non riesce. Per informazioni sugli aggiornamenti di sistema, consultare la pagina man "cluster image".

Onboard Key Manager memorizza le chiavi nella memoria volatile. I contenuti della memoria volatile vengono cancellati quando il sistema viene riavviato o arrestato. In condizioni operative normali, il contenuto della memoria volatile viene cancellato entro 30 secondi quando il sistema viene arrestato.

Prima di iniziare

- Se si utilizza NSE con un server KMIP (Key Management) esterno, è necessario eliminare il database del gestore delle chiavi esterno.

  "Passaggio alla gestione delle chiavi integrata dalla gestione delle chiavi esterna"

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare il Gestore chiavi integrato.

Fasi

1. Avviare il comando di configurazione del gestore delle chiavi:

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

> Impostare `cc-mode-enabled=yes` per richiedere agli utenti di inserire la passphrase del gestore delle chiavi dopo un riavvio. Il `- cc-mode-enabled` L'opzione non è supportata nelle configurazioni MetroCluster. Il `security key-manager onboard enable` il comando sostituisce `security key-manager setup` comando.

Nell'esempio seguente viene avviato il comando di configurazione del gestore delle chiavi sul cluster1 senza che sia necessario inserire la passphrase dopo ogni riavvio:

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Al prompt della passphrase, immettere una passphrase compresa tra 32 e 256 caratteri oppure, per "cc-mode", una passphrase compresa tra 64 e 256 caratteri.

> Se la passphrase "cc-mode" specificata è inferiore a 64 caratteri, si verifica un ritardo di cinque secondi prima che l'operazione di configurazione del gestore delle chiavi visualizzi nuovamente il prompt della passphrase.

3. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.
4. Verificare che le chiavi di autenticazione siano state create:

```
security key-manager key query -node node
```

> Il `security key-manager key query` il comando sostituisce `security key-manager query key` comando. Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene verificata la creazione di chiavi di autenticazione per `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: onboard
          Node: node1

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Al termine

Copiare la passphrase in una posizione sicura all'esterno del sistema di storage per utilizzarla in futuro.

Viene eseguito automaticamente il backup di tutte le informazioni di gestione delle chiavi nel database replicato (RDB) del cluster. È inoltre necessario eseguire il backup manuale delle informazioni per utilizzarle in caso di disastro.

Abilitare la gestione delle chiavi integrata in ONTAP 9.5 e versioni precedenti

È possibile utilizzare Onboard Key Manager per autenticare i nodi del cluster su un disco FIPS o SED. Onboard Key Manager è uno strumento integrato che fornisce chiavi di autenticazione ai nodi dello stesso sistema storage dei dati. Onboard Key Manager è conforme a FIPS-140-2 livello 1.

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati

crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

A proposito di questa attività

È necessario eseguire `security key-manager setup` ogni volta che si aggiunge un nodo al cluster.

Se si dispone di una configurazione MetroCluster, consultare le seguenti linee guida:

- In ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale e. `security key-manager setup -sync-metrocluster-config yes` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.
- Prima di ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale, attendere circa 20 secondi, quindi eseguire `security key-manager setup` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente. Per `volume create`, non è necessario specificare `-encrypt true`. Per `volume move start`, non è necessario specificare `-encrypt-destination true`.

> Dopo un tentativo di passphrase non riuscito, riavviare nuovamente il nodo.

Prima di iniziare

- Se si utilizza NSE con un server KMIP (Key Management) esterno, è necessario eliminare il database del gestore delle chiavi esterno.

  "Passaggio alla gestione delle chiavi integrata dalla gestione delle chiavi esterna"

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare il Gestore chiavi integrato.

Fasi

1. Avviare la configurazione di Key Manager:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   > A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase del gestore delle chiavi dopo un riavvio. Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e. `volume move start` i comandi vengono crittografati automaticamente.

   Nell'esempio seguente viene avviata l'impostazione del gestore delle chiavi sul cluster1 senza che sia necessario inserire la passphrase dopo ogni riavvio:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Invio `yes` quando viene richiesto di configurare la gestione delle chiavi integrata.
3. Al prompt della passphrase, immettere una passphrase compresa tra 32 e 256 caratteri oppure, per “cc-mode”, una passphrase compresa tra 64 e 256 caratteri.

> Se la passphrase “cc-mode” specificata è inferiore a 64 caratteri, si verifica un ritardo di cinque secondi prima che l’operazione di configurazione del gestore delle chiavi visualizzi nuovamente il prompt della passphrase.

4. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.
5. Verificare che le chiavi siano configurate per tutti i nodi:

   `security key-manager key show`

   Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

Al termine

Viene eseguito automaticamente il backup di tutte le informazioni di gestione delle chiavi nel database replicato (RDB) del cluster.

Ogni volta che si configura la passphrase di Onboard Key Manager, è necessario eseguire il backup manuale delle informazioni in una posizione sicura all'esterno del sistema di storage per l'utilizzo in caso di disastro. Vedere "Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate".

Assegnazione di una chiave di autenticazione dei dati a un'unità FIPS o SED (onboard key management)

È possibile utilizzare `storage encryption disk modify` Comando per assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED. I nodi del cluster utilizzano questa chiave per accedere ai dati sul disco.

A proposito di questa attività

Un'unità con crittografia automatica è protetta da accessi non autorizzati solo se l'ID della chiave di autenticazione è impostato su un valore non predefinito. L'ID sicuro del produttore (MSID), con ID chiave 0x0, è il valore predefinito standard per i dischi SAS. Per i dischi NVMe, il valore predefinito standard è una chiave nulla, rappresentata come ID chiave vuoto. Quando si assegna l'ID della chiave a un'unità con crittografia automatica, il sistema modifica l'ID della chiave di autenticazione in un valore non predefinito.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fasi

1. Assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED:

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

   Per la sintassi completa dei comandi, vedere la pagina man del comando.

   > È possibile utilizzare `security key-manager key query -key-type NSE-AK` Per visualizzare gli ID chiave.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   00000000000000000200000000000010019215b9738bc7b43d4698c80246db1f4

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

2. Verificare che le chiavi di autenticazione siano state assegnate:

   `storage encryption disk show`

   Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

Assegnare una chiave di autenticazione FIPS 140-2 a un disco FIPS

È possibile utilizzare `storage encryption disk modify` con il `-fips-key-id` Opzione per assegnare una chiave di autenticazione FIPS 140-2 a un disco FIPS. I nodi del cluster utilizzano questa chiave per operazioni di guida diverse dall'accesso ai dati, come la prevenzione di attacchi di tipo Denial-of-service sul disco.

A proposito di questa attività

La configurazione della sicurezza potrebbe richiedere l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

Questa procedura non comporta interruzioni.

Prima di iniziare

Il firmware del disco deve supportare la conformità FIPS 140-2. Il "Tool di matrice di interoperabilità NetApp" contiene informazioni sulle versioni del firmware del disco supportate.

Fasi

1. Assicurarsi di aver assegnato una chiave di autenticazione dei dati. Questa operazione può essere eseguita utilizzando un gestore delle chiavi esterno o un gestore delle chiavi integrato. Verificare che il tasto sia assegnato con il comando `storage encryption disk show`.
2. Assegnare una chiave di autenticazione FIPS 140-2 ai SED:

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

   È possibile utilizzare `security key-manager query` Per visualizzare gli ID chiave.

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
   6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

3. Verificare che la chiave di autenticazione sia stata assegnata:

   ```
   storage encryption disk show -fips
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   ```
   cluster1::> storage encryption disk show -fips
   Disk    Mode FIPS-Compliance Key ID
   ------  ----
   ------------------------------------------------------------------
   2.10.0  full
   6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
   2.10.1  full
   6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
   [...]
   ```

Abilitare la modalità compatibile con FIPS a livello di cluster per le connessioni al server KMIP

È possibile utilizzare `security config modify` con il `-is-fips-enabled` Opzione per abilitare la modalità compatibile con FIPS a livello di cluster per i dati in volo. In questo modo, il cluster utilizza OpenSSL in modalità FIPS durante la connessione ai server KMIP.

A proposito di questa attività

Quando si attiva la modalità compatibile con FIPS a livello di cluster, il cluster utilizza automaticamente solo le suite di crittografia convalidate da TLS1.2 e FIPS. La modalità compatibile con FIPS a livello di cluster è disattivata per impostazione predefinita.

È necessario riavviare manualmente i nodi del cluster dopo aver modificato la configurazione di sicurezza a livello di cluster.

Prima di iniziare

- Lo storage controller deve essere configurato in modalità conforme a FIPS.
- Tutti i server KMIP devono supportare TLSv1.2. Il sistema richiede TLSv1.2 per completare la connessione al server KMIP quando è attivata la modalità compatibile con FIPS a livello di cluster.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Verificare che TLSv1.2 sia supportato:

   ```
   security config show -supported-protocols
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. Abilitare la modalità compatibile con FIPS a livello di cluster:

   `security config modify -is-fips-enabled true -interface SSL`

   Per la sintassi completa dei comandi, vedere la pagina man.

4. Riavviare manualmente i nodi del cluster.
5. Verificare che la modalità compatibile con FIPS a livello di cluster sia attivata:

   `security config show`

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL:!RC4
```

Gestire la crittografia NetApp

Decrittografare i dati del volume

È possibile utilizzare `volume move start` comando per spostare e rimuovere la crittografia dei dati del volume.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster. In alternativa, puoi essere un amministratore SVM a cui l'amministratore del cluster ha delegato l'autorità. Per ulteriori informazioni, vedere "Delegare l'autorità per eseguire il comando di spostamento del volume".

Fasi

1. Spostare un volume crittografato esistente e annullare la crittografia dei dati sul volume:

   `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

   Per la sintassi completa dei comandi, vedere la pagina man del comando.

   Il seguente comando sposta un volume esistente denominato `vol1` all'aggregato di destinazione `aggr3` e annulla la crittografia dei dati sul volume:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   Il sistema elimina la chiave di crittografia per il volume. I dati del volume non sono crittografati.

2. Verificare che il volume sia disattivato per la crittografia:

   `volume show -encryption`

   Per la sintassi completa dei comandi, vedere la pagina man del comando.

   Il seguente comando indica se i volumi sono accesi `cluster1` sono crittografati:

   ```
   cluster1::> volume show -encryption

   Vserver  Volume   Aggregate   State    Encryption State
   -------  ------   ---------   -----    ----------------
   vs1      vol1     aggr1       online   none
   ```

Spostare un volume crittografato

È possibile utilizzare `volume move start` comando per spostare un volume crittografato. Il volume spostato può risiedere sullo stesso aggregato o su un aggregato diverso.

A proposito di questa attività

Lo spostamento non riesce se il nodo di destinazione o il volume di destinazione non supporta la crittografia del volume.

Il `-encrypt-destination` opzione per `volume move start` l'impostazione predefinita è true per i volumi crittografati. Il requisito di specificare che non si desidera che il volume di destinazione venga crittografato garantisce che i dati sul volume non vengano inavvertitamente decrittografati.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster. In alternativa, puoi essere un amministratore SVM a cui l'amministratore del cluster ha delegato l'autorità. Per ulteriori informazioni, vedere "delegare l'autorità per eseguire il comando di spostamento del volume".

Fasi

1. Spostare un volume crittografato esistente e lasciare crittografati i dati sul volume:

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`*

   Per la sintassi completa dei comandi, vedere la pagina man del comando.

   Il seguente comando sposta un volume esistente denominato `vol1` all'aggregato di destinazione `aggr3` e lascia crittografati i dati sul volume:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. Verificare che il volume sia abilitato per la crittografia:

   `volume show -is-encrypted true`

   Per la sintassi completa dei comandi, vedere la pagina man del comando.

   Il seguente comando visualizza i volumi crittografati su `cluster1`:

   ```
   cluster1::> volume show -is-encrypted true

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   -------  ------  ---------  -----  ----  -----  --------- ----
   vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
   ```

Delegare l'autorità per eseguire il comando di spostamento del volume

È possibile utilizzare `volume move` comando per crittografare un volume esistente, spostare un volume crittografato o annullare la crittografia di un volume. Gli amministratori del cluster possono eseguire `volume move` Oppure possono delegare l'autorità per eseguire il comando agli amministratori SVM.

A proposito di questa attività

Per impostazione predefinita, agli amministratori SVM viene assegnato il `vsadmin` ruolo, che non include l'autorità per spostare i volumi. È necessario assegnare `vsadmin-volume` Agli amministratori di SVM per consentire loro di eseguire `volume move` comando.

Fase

1. Delegare l'autorità per eseguire `volume move` comando:

   `security login modify -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`vsadmin-volume`*

Per la sintassi completa dei comandi, vedere la pagina man del comando.

Il seguente comando concede all'amministratore SVM l'autorizzazione per eseguire `volume move` comando.

```
cluster1::>security login modify -vserver engData -user-or-group-name
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

Modificare la chiave di crittografia per un volume con il comando di avvio della chiave di crittografia del volume

È consigliabile modificare periodicamente la chiave di crittografia di un volume. A partire da ONTAP 9.3, è possibile utilizzare `volume encryption rekey start` per modificare la chiave di crittografia.

A proposito di questa attività

Una volta avviata un'operazione di rekey, questa deve essere completata. Non è possibile tornare alla vecchia chiave. Se si verificano problemi di prestazioni durante l'operazione, è possibile eseguire `volume encryption rekey pause` per sospendere l'operazione e il `volume encryption rekey resume` per riprendere l'operazione.

Fino al termine dell'operazione di rekey, il volume avrà due tasti. Le nuove scritture e le corrispondenti letture utilizzeranno la nuova chiave. In caso contrario, Read utilizzerà la vecchia chiave.

> Non è possibile utilizzare `volume encryption rekey start` Per modificare la chiave di un volume SnapLock.

Fasi

1. Modifica di una chiave di crittografia:

   `volume encryption rekey start -vserver SVM_name -volume volume_name`

   Il seguente comando modifica la chiave di crittografia per `vol1` Su SVM`vs1`:

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. Verificare lo stato dell'operazione di rekey:

   `volume encryption rekey show`

   Per la sintassi completa dei comandi, vedere la pagina man del comando.

   Il seguente comando visualizza lo stato dell'operazione di rekey:

```
cluster1::> volume encryption rekey show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   ---------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. Una volta completata l'operazione di rekey, verificare che il volume sia abilitato per la crittografia:

   `volume show -is-encrypted true`

   Per la sintassi completa dei comandi, vedere la pagina man del comando.

   Il seguente comando visualizza i volumi crittografati su `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Modificare la chiave di crittografia per un volume con il comando di avvio spostamento volume

È consigliabile modificare periodicamente la chiave di crittografia di un volume. È possibile utilizzare `volume move start` per modificare la chiave di crittografia. È necessario utilizzare `volume move start` In ONTAP 9.2 e versioni precedenti. Il volume spostato può risiedere sullo stesso aggregato o su un aggregato diverso.

A proposito di questa attività

Non è possibile utilizzare `volume move start` Per modificare la chiave di un volume SnapLock o FlexGroup.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster. In alternativa, puoi essere un amministratore SVM a cui l'amministratore del cluster ha delegato l'autorità. Per ulteriori informazioni, vedere "delegare l'autorità per eseguire il comando di spostamento del volume".

Fasi

1. Spostare un volume esistente e modificare la chiave di crittografia:

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

   Per la sintassi completa dei comandi, vedere la pagina man del comando.

   Il seguente comando sposta un volume esistente denominato **`vol1`** all'aggregato di destinazione **`aggr2`** e modifica la chiave di crittografia:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -generate-destination-key true
```

Viene creata una nuova chiave di crittografia per il volume. I dati sul volume rimangono crittografati.

2. Verificare che il volume sia abilitato per la crittografia:

   `volume show -is-encrypted true`

   Per la sintassi completa dei comandi, vedere la pagina man del comando.

   Il seguente comando visualizza i volumi crittografati su `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Ruotare le chiavi di autenticazione per NetApp Storage Encryption

È possibile ruotare le chiavi di autenticazione quando si utilizza NetApp Storage Encryption (NSE).

A proposito di questa attività

La rotazione delle chiavi di autenticazione in un ambiente NSE è supportata se si utilizza External Key Manager (KMIP).

> La rotazione delle chiavi di autenticazione in un ambiente NSE non è supportata da Onboard Key Manager (OKM).

Fasi

1. Utilizzare `security key-manager create-key` per generare nuove chiavi di autenticazione.

   Prima di poter modificare le chiavi di autenticazione, è necessario generare nuove chiavi di autenticazione.

2. Utilizzare `storage encryption disk modify -disk * -data-key-id` per modificare le chiavi di autenticazione.

Eliminare un volume crittografato

È possibile utilizzare `volume delete` comando per eliminare un volume crittografato.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster. In alternativa, puoi essere un amministratore SVM a cui l'amministratore del cluster ha delegato l'autorità. Per ulteriori informazioni, vedere "delegare l'autorità per eseguire il comando di spostamento del volume".

- Il volume deve essere offline.

Fase

1. Eliminazione di un volume crittografato:

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

   Per la sintassi completa dei comandi, vedere la pagina man del comando.

   Il seguente comando elimina un volume crittografato denominato `vol1`:

   ```
   cluster1::> volume delete -vserver vs1 -volume vol1
   ```

   Invio `yes` quando viene richiesto di confermare l'eliminazione.

   Il sistema elimina la chiave di crittografia per il volume dopo 24 ore.

   Utilizzare `volume delete` con `-force true` opzione per eliminare un volume e distruggere immediatamente la chiave di crittografia corrispondente. Questo comando richiede privilegi avanzati. Per ulteriori informazioni, consulta la pagina man.

Al termine

È possibile utilizzare `volume recovery-queue` comando per ripristinare un volume cancellato durante il periodo di conservazione dopo l'emissione di `volume delete` comando:

`volume recovery-queue` *`SVM_name`* `-volume` *`volume_name`*

"Come utilizzare la funzione Volume Recovery (Ripristino volume)"

Eliminare in modo sicuro i dati su un volume crittografato

Elimina in modo sicuro i dati su una panoramica dei volumi crittografati

A partire da ONTAP 9.4, è possibile utilizzare l'eliminazione sicura per eseguire lo scrubbing dei dati senza interruzioni su volumi abilitati per NVE. Lo scrubbing dei dati su un volume crittografato garantisce che non sia possibile ripristinarli dal supporto fisico, ad esempio in caso di "ssaccheggio", in cui le tracce dei dati potrebbero essere state lasciate indietro quando i blocchi sono stati sovrascritti o per eliminare in modo sicuro i dati di un tenant vuoto.

L'eliminazione sicura funziona solo per i file precedentemente cancellati sui volumi abilitati per NVE. Non è possibile eseguire lo scrubbing di un volume non crittografato. È necessario utilizzare i server KMIP per fornire le chiavi, non il gestore delle chiavi integrato.

Considerazioni per l'utilizzo della rimozione sicura

- I volumi creati in un aggregato abilitato per NetApp aggregate Encryption (NAE) non supportano l'eliminazione sicura.
- L'eliminazione sicura funziona solo per i file precedentemente cancellati sui volumi abilitati per NVE.

- Non è possibile eseguire lo scrubbing di un volume non crittografato.
- È necessario utilizzare i server KMIP per fornire le chiavi, non il gestore delle chiavi integrato.

L'eliminazione sicura funziona in modo diverso a seconda della versione di ONTAP in uso.

ONTAP 9.8 e versioni successive

- L'eliminazione sicura è supportata da MetroCluster e FlexGroup.
- Se il volume da rimuovere è l'origine di una relazione SnapMirror, non è necessario interrompere la relazione SnapMirror per eseguire un'eliminazione sicura.
- Il metodo di ricEncryption è diverso per i volumi che utilizzano la protezione dei dati SnapMirror rispetto ai volumi che non utilizzano la protezione dei dati SnapMirror o quelli che utilizzano la protezione estesa dei dati SnapMirror.
  - Per impostazione predefinita, i volumi che utilizzano la modalità di protezione dati SnapMirror (DP) crittografano nuovamente i dati utilizzando il metodo di ricifratura dello spostamento del volume.
  - Per impostazione predefinita, i volumi che non utilizzano la protezione dei dati SnapMirror o i volumi che utilizzano la modalità XDP (Extended Data Protection) di SnapMirror utilizzano il metodo di riscrittazione in-place.
  - È possibile modificare queste impostazioni predefinite utilizzando `secure purge re-encryption-method [volume-move|in-place-rekey]` comando.
- Per impostazione predefinita, tutte le copie Snapshot nei volumi FlexVol vengono eliminate automaticamente durante l'operazione di eliminazione sicura. Per impostazione predefinita, le istantanee nei volumi e nei volumi FlexGroup che utilizzano la protezione dei dati SnapMirror non vengono eliminate automaticamente durante l'operazione di eliminazione sicura. È possibile modificare queste impostazioni predefinite utilizzando `secure purge delete-all-snapshots [true|false]` comando.

ONTAP 9.7 e versioni precedenti:

- L'eliminazione sicura non supporta quanto segue:
  - FlexClone
  - SnapVault
  - FabricPool
- Se il volume da rimuovere è l'origine di una relazione SnapMirror, è necessario interrompere la relazione SnapMirror prima di poter eliminare il volume.

  Se nel volume sono presenti copie Snapshot occupate, è necessario rilasciare le copie Snapshot prima di poter eliminare il volume. Ad esempio, potrebbe essere necessario separare un volume FlexClone dal volume padre.

- Il corretto richiamo della funzione di eliminazione sicura attiva uno spostamento del volume che crittografa nuovamente i dati rimanenti non eliminati con una nuova chiave.

  Il volume spostato rimane nell'aggregato corrente. La vecchia chiave viene automaticamente distrutta, garantendo che i dati rimossi non possano essere ripristinati dal supporto di storage.

Eliminazione sicura dei dati su un volume crittografato senza una relazione SnapMirror

A partire da ONTAP 9.4, è possibile utilizzare la funzione Secure-purge per i dati “scrub” senza interruzioni su volumi abilitati per NVE.

A proposito di questa attività

Il completamento dell’eliminazione sicura può richiedere da diversi minuti a molte ore, a seconda della quantità di dati contenuti nei file cancellati. È possibile utilizzare `volume encryption secure-purge show` per visualizzare lo stato dell’operazione. È possibile utilizzare `volume encryption secure-purge abort` per terminare l’operazione.

> Per eseguire un’eliminazione sicura su un host SAN, è necessario eliminare l’intero LUN contenente i file da eliminare oppure è necessario essere in grado di perforare i LUN per i blocchi che appartengono ai file che si desidera eliminare. Se non è possibile eliminare il LUN o se il sistema operativo host non supporta i fori di punzonatura nel LUN, non è possibile eseguire un’eliminazione sicura.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Per questa attività sono richiesti privilegi avanzati.

Fasi

1. Eliminare i file o il LUN che si desidera eliminare in modo sicuro.
   - Su un client NAS, eliminare i file che si desidera eliminare in modo sicuro.
   - Su un host SAN, eliminare il LUN che si desidera eliminare in modo sicuro o perforare i fori nel LUN per i blocchi che appartengono ai file che si desidera eliminare.
2. Sul sistema storage, passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

3. Se i file che si desidera eliminare in modo sicuro si trovano in snapshot, eliminare le snapshot:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. Eliminare in modo sicuro i file cancellati:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   Il seguente comando elimina in modo sicuro i file cancellati su `vol1` Su SVM`vs1`:

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. Verificare lo stato dell’operazione di eliminazione sicura:

   ```
   volume encryption secure-purge show
   ```

Eliminare in modo sicuro i dati su un volume crittografato con una relazione asincrona SnapMirror

A partire da ONTAP 9.8, è possibile utilizzare un purge sicuro per i dati “scrub” senza interruzioni su volumi abilitati per NVE con una relazione asincrona SnapMirror.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Per questa attività sono richiesti privilegi avanzati.

A proposito di questa attività

Il completamento dell’eliminazione sicura può richiedere da diversi minuti a molte ore, a seconda della quantità di dati contenuti nei file cancellati. È possibile utilizzare `volume encryption secure-purge show` per visualizzare lo stato dell’operazione. È possibile utilizzare `volume encryption secure-purge abort` per terminare l’operazione.

> Per eseguire un’eliminazione sicura su un host SAN, è necessario eliminare l’intero LUN contenente i file da eliminare oppure è necessario essere in grado di perforare i LUN per i blocchi che appartengono ai file che si desidera eliminare. Se non è possibile eliminare il LUN o se il sistema operativo host non supporta i fori di punzonatura nel LUN, non è possibile eseguire un’eliminazione sicura.

Fasi

1. Nel sistema di archiviazione, passare al livello di privilegi avanzato:

   ```
   set -privilege advanced
   ```

2. Eliminare i file o il LUN che si desidera eliminare in modo sicuro.
   - Su un client NAS, eliminare i file che si desidera eliminare in modo sicuro.
   - Su un host SAN, eliminare il LUN che si desidera eliminare in modo sicuro o perforare i fori nel LUN per i blocchi che appartengono ai file che si desidera eliminare.
3. Preparare il volume di destinazione nella relazione asincrona per la rimozione sicura:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Ripetere questo passaggio su ciascun volume nella relazione di SnapMirror asincrona.

4. Se i file che si desidera eliminare in modo sicuro si trovano nelle copie Snapshot, eliminare le copie Snapshot:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. Se i file che si desidera eliminare in modo sicuro si trovano nelle copie Snapshot di base, procedere come segue:

   a. Creare una copia Snapshot sul volume di destinazione nella relazione SnapMirror asincrona:

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. Aggiornare SnapMirror per spostare in avanti la copia Snapshot di base:

```
snapmirror update -source-snapshot snapshot_name -destination-path
destination_path
```

Ripetere questo passaggio per ogni volume nella relazione di SnapMirror asincrona.

a. Ripetere i passaggi (a) e (b) pari al numero di copie Snapshot di base più una.

   Ad esempio, se si dispone di due copie Snapshot di base, ripetere i passaggi (a) e (b) tre volte.

b. Verificare che la copia Snapshot di base sia presente:

```
snapshot show -vserver SVM_name -volume volume_name
```

c. Eliminare la copia Snapshot di base:

```
snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot
```

6. Eliminare in modo sicuro i file cancellati:

```
volume encryption secure-purge start -vserver svm_name -volume volume_name
```

   Ripetere questo passaggio su ciascun volume nella relazione di SnapMirror asincrona.

   Il seguente comando elimina in modo sicuro i file cancellati su “vol1” su SVM “vs1”:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. Verificare lo stato dell’operazione di eliminazione sicura:

```
volume encryption secure-purge show
```

Eseguire lo scrubbing dei dati su un volume crittografato con una relazione SnapMirror sincrona

A partire da ONTAP 9,8, puoi utilizzare una pulizia sicura per "scrub" senza interruzioni dei dati su volumi abilitati per NVE con una relazione di SnapMirror sincrono.

A proposito di questa attività

Il completamento di una rimozione sicura potrebbe richiedere da diversi minuti a molte ore, a seconda della quantità di dati contenuti nei file cancellati. È possibile utilizzare `volume encryption secure-purge show` per visualizzare lo stato dell’operazione. È possibile utilizzare `volume encryption secure-purge abort` per terminare l’operazione.

> Per eseguire un’eliminazione sicura su un host SAN, è necessario eliminare l’intero LUN contenente i file da eliminare oppure è necessario essere in grado di perforare i LUN per i blocchi che appartengono ai file che si desidera eliminare. Se non è possibile eliminare il LUN o se il sistema operativo host non supporta i fori di punzonatura nel LUN, non è possibile eseguire un’eliminazione sicura.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.

- Per questa attività sono richiesti privilegi avanzati.

Fasi

1. Sul sistema storage, passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Eliminare i file o il LUN che si desidera eliminare in modo sicuro.
   - Su un client NAS, eliminare i file che si desidera eliminare in modo sicuro.
   - Su un host SAN, eliminare il LUN che si desidera eliminare in modo sicuro o perforare i fori nel LUN per i blocchi che appartengono ai file che si desidera eliminare.

3. Preparare il volume di destinazione nella relazione asincrona per la rimozione sicura:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Ripetere questo passaggio per l'altro volume nella relazione di Synchronous SnapMirror.

4. Se i file che si desidera eliminare in modo sicuro si trovano nelle copie Snapshot, eliminare le copie Snapshot:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

5. Se il file di eliminazione sicuro si trova nelle copie Snapshot di base o comuni, aggiornare SnapMirror per spostare la copia Snapshot comune in avanti:

   ```
   snapmirror update -source-snapshot snapshot_name -destination-path
   destination_path
   ```

   Esistono due copie Snapshot comuni, quindi questo comando deve essere emesso due volte.

6. Se il file di eliminazione sicuro si trova nella copia Snapshot coerente con l'applicazione, eliminare la copia Snapshot su entrambi i volumi nella relazione SnapMirror sincrona:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

   Eseguire questa operazione su entrambi i volumi.

7. Eliminare in modo sicuro i file cancellati:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   Ripetere questo passaggio su ciascun volume nella relazione SnapMirror sincrona.

   Il seguente comando elimina in modo sicuro i file cancellati su "vol1" su SMV "vs1".

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. Verificare lo stato dell'operazione di eliminazione sicura:

```
volume encryption secure-purge show
```

Modificare la passphrase di gestione della chiave integrata

È consigliabile modificare periodicamente la passphrase di gestione delle chiavi integrate. Copiare la nuova passphrase di gestione della chiave integrata in una posizione sicura all'esterno del sistema di storage per un utilizzo futuro.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- Per questa attività sono richiesti privilegi avanzati.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Modificare la passphrase di gestione della chiave integrata:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 e versioni successive	`security key-manager onboard update-passphrase`
ONTAP 9.5 e versioni precedenti	`security key-manager update-passphrase`

   Per la sintassi completa dei comandi, vedere le pagine man.

   Il seguente comando ONTAP 9.6 consente di modificare la passphrase di gestione delle chiavi integrata per `cluster1`:

   ```
   cluster1::> security key-manager onboard update-passphrase
   Warning: This command will reconfigure the cluster passphrase for
   onboard key management for Vserver "cluster1".
   Do you want to continue? {y|n}: y
   Enter current passphrase:
   Enter new passphrase:
   ```

3. Invio `y` quando viene richiesto di modificare la passphrase di gestione della chiave integrata.
4. Inserire la passphrase corrente al prompt della passphrase corrente.
5. Al prompt della nuova passphrase, immettere una passphrase compresa tra 32 e 256 caratteri oppure, per "cc-mode", una passphrase compresa tra 64 e 256 caratteri.

   Se la passphrase "cc-mode" specificata è inferiore a 64 caratteri, si verifica un ritardo di cinque secondi prima che l'operazione di configurazione del gestore delle chiavi visualizzi nuovamente il prompt della

passphrase.

6. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.

Al termine

In un ambiente MetroCluster, è necessario aggiornare la passphrase sul cluster partner:

- In ONTAP 9.5 e versioni precedenti, è necessario eseguire `security key-manager update-passphrase` con la stessa passphrase sul cluster partner.
- In ONTAP 9.6 e versioni successive, viene richiesto di eseguire `security key-manager onboard sync` con la stessa passphrase sul cluster partner.

Copiare la passphrase di gestione della chiave integrata in una posizione sicura all'esterno del sistema di storage per un utilizzo futuro.

È necessario eseguire il backup manuale delle informazioni di gestione delle chiavi ogni volta che si modifica la passphrase di gestione delle chiavi integrata.

"Backup manuale delle informazioni di gestione delle chiavi integrate"

Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate

Ogni volta che si configura la passphrase di Onboard Key Manager, è necessario copiare le informazioni di gestione delle chiavi integrate in una posizione sicura all'esterno del sistema di storage.

Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Per questa attività sono richiesti privilegi avanzati.

A proposito di questa attività

Viene eseguito automaticamente il backup di tutte le informazioni di gestione delle chiavi nel database replicato (RDB) del cluster. È inoltre necessario eseguire il backup manuale delle informazioni di gestione delle chiavi per utilizzarle in caso di disastro.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Visualizzare le informazioni di backup della gestione delle chiavi per il cluster:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 e versioni successive	`security key-manager onboard show-backup`
ONTAP 9.5 e versioni precedenti	`security key-manager backup show`

Per la sintassi completa dei comandi, vedere le pagine man.

+ il seguente comando 9.6 visualizza le informazioni di backup per la gestione delle chiavi per `cluster1`:

+

```
cluster1::> security key-manager onboard show-backup

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
     IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAIAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAACgAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAoAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAACQAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

1. Copiare le informazioni di backup in una posizione sicura all’esterno del sistema di storage per utilizzarle in caso di disastro.

Ripristinare le chiavi di crittografia integrate per la gestione delle chiavi

La procedura che segui per ripristinare le chiavi di crittografia della gestione delle chiavi integrate varia in base alla tua versione di ONTAP.

Prima di iniziare

- Se si utilizza NSE con un server KMIP (Key Management) esterno, è necessario eliminare il database del gestore delle chiavi esterno. Per ulteriori informazioni, vedere "transizione alla gestione delle chiavi integrata dalla gestione delle chiavi esterna"
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

> Se stai utilizzando NSE su un sistema con un modulo Flash cache, dovresti abilitare anche NVE o NAE. NSe non crittografa i dati che risiedono nel modulo Flash cache.

ONTAP 9,8 e versioni successive con volume root crittografato

> Se si esegue ONTAP 9,8 o versione successiva e il volume root non è crittografato, seguire la procedura per ONTAP 9,6 o versione successiva.

Se si utilizza ONTAP 9.8 e versioni successive e il volume root è crittografato, è necessario impostare una passphrase di ripristino per la gestione delle chiavi integrata nel menu di avvio. Questo processo è necessario anche se si esegue una sostituzione dei supporti di avvio.

1. Avviare il nodo dal menu di boot e selezionare l'opzione `(10) Set onboard key management recovery secrets`.
2. Invio `y` per utilizzare questa opzione.
3. Quando richiesto, inserire la passphrase di gestione della chiave integrata per il cluster.
4. Quando richiesto, inserire i dati della chiave di backup.

   Il nodo torna al menu di boot.

5. Dal menu di avvio, selezionare opzione `(1) Normal Boot`.

ONTAP 9.6 e versioni successive

1. Verificare che la chiave debba essere ripristinata:
   `security key-manager key query -node` *`node`*
2. Ripristinare la chiave:
   `security key-manager onboard sync`

   Per la sintassi completa dei comandi, vedere le pagine man.

   Il seguente comando ONTAP 9.6 sincronizza le chiavi nella gerarchia di chiavi integrate:

   ```
   cluster1::> security key-manager onboard sync

   Enter the cluster-wide passphrase for onboard key management in Vserver
   "cluster1"::    <32..256 ASCII characters long text>
   ```

3. Al prompt della passphrase, inserire la passphrase di gestione della chiave integrata per il cluster.

ONTAP 9.5 e versioni precedenti

1. Verificare che la chiave debba essere ripristinata:

```
security key-manager key show
```

2. Se si utilizza ONTAP 9.8 e versioni successive e il volume root è crittografato, attenersi alla seguente procedura:

   Se si utilizza ONTAP 9.6 o 9.7, o se si utilizza ONTAP 9.8 o versione successiva e il volume root non è crittografato, ignorare questo passaggio.

3. Ripristinare la chiave:
   `security key-manager setup -node node`

   Per la sintassi completa dei comandi, vedere le pagine man.

4. Al prompt della passphrase, inserire la passphrase di gestione della chiave integrata per il cluster.

Ripristinare le chiavi di crittografia esterne per la gestione delle chiavi

È possibile ripristinare manualmente le chiavi di crittografia della gestione esterna delle chiavi e inviarle a un nodo diverso. Questa operazione potrebbe essere utile se si sta riavviando un nodo temporaneamente inattivo quando sono state create le chiavi per il cluster.

A proposito di questa attività

In ONTAP 9.6 e versioni successive, è possibile utilizzare `security key-manager key query -node node_name` per verificare se la chiave deve essere ripristinata.

In ONTAP 9.5 e versioni precedenti, è possibile utilizzare `security key-manager key show` per verificare se la chiave deve essere ripristinata.

> Se stai utilizzando NSE su un sistema con un modulo Flash cache, dovresti abilitare anche NVE o NAE. NSe non crittografa i dati che risiedono nel modulo Flash cache.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

Fasi

1. Se si utilizza ONTAP 9.8 o versione successiva e il volume root è crittografato, procedere come segue:

   Se si utilizza ONTAP 9.7 o versioni precedenti o se si utilizza ONTAP 9.8 o versioni successive e il volume root non è crittografato, ignorare questo passaggio.

   a. Impostare il bootargs:
      ```
      setenv kmip.init.ipaddr <ip-address>+
      setenv kmip.init.netmask <netmask>+
      setenv kmip.init.gateway <gateway>+
      setenv kmip.init.interface e0M+
      boot_ontap
      ```
   b. Avviare il nodo dal menu di boot e selezionare l'opzione `(11) Configure node for external key management`.
   c. Seguire le istruzioni per inserire il certificato di gestione.

Una volta inserite tutte le informazioni del certificato di gestione, il sistema torna al menu di avvio.

d. Dal menu di avvio, selezionare opzione `(1) Normal Boot`.

2. Ripristinare la chiave:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 e versioni successive	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5 e versioni precedenti

> `node` per impostazione predefinita, tutti i nodi. Per la sintassi completa dei comandi, vedere le pagine man. Questo comando non è supportato quando è attivata la gestione delle chiavi integrate.

Il seguente comando ONTAP 9.6 ripristina le chiavi di autenticazione esterne per la gestione delle chiavi in tutti i nodi in `cluster1`:

```
cluster1::> security key-manager external restore
```

Sostituire i certificati SSL

Tutti i certificati SSL hanno una data di scadenza. È necessario aggiornare i certificati prima che scadano per evitare la perdita di accesso alle chiavi di autenticazione.

Prima di iniziare

- È necessario aver ottenuto il certificato pubblico e la chiave privata sostitutivi per il cluster (certificato del client KMIP).
- È necessario aver ottenuto il certificato pubblico sostitutivo per il server KMIP (certificato KMIP server-ca).
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- In un ambiente MetroCluster, è necessario sostituire il certificato SSL KMIP su entrambi i cluster.

> È possibile installare i certificati client e server sostitutivi sul server KMIP prima o dopo l'installazione dei certificati sul cluster.

Fasi

1. Installare il nuovo certificato KMIP server-ca:

```
security certificate install -type server-ca -vserver <>
```

2. Installare il nuovo certificato del client KMIP:

```
security certificate install -type client -vserver <>
```

3. Aggiornare la configurazione del gestore delle chiavi per utilizzare i certificati appena installati:

```
security key-manager external modify -vserver <> -client-cert <> -server-ca
-certs <>
```

Se si esegue ONTAP 9.6 o versione successiva in un ambiente MetroCluster e si desidera modificare la configurazione del gestore delle chiavi nella SVM amministrativa, è necessario eseguire il comando su entrambi i cluster della configurazione.

> L'aggiornamento della configurazione del gestore delle chiavi per utilizzare i certificati appena installati restituisce un errore se le chiavi pubbliche/private del nuovo certificato client sono diverse dalle chiavi installate in precedenza. Consultare l'articolo della Knowledge base "Le chiavi pubbliche o private del nuovo certificato client sono diverse dal certificato client esistente" per istruzioni su come ignorare questo errore.

Sostituire un'unità FIPS o SED

È possibile sostituire un'unità FIPS o SED nello stesso modo in cui si sostituisce un disco normale. Assicurarsi di assegnare nuove chiavi di autenticazione dei dati all'unità sostitutiva. Per un'unità FIPS, potrebbe essere necessario assegnare una nuova chiave di autenticazione FIPS 140-2.

> Se è in uso una coppia ha "Crittografia dei dischi SAS o NVMe (SED, NSE, FIPS)", è necessario seguire le istruzioni riportate nell'argomento "Ripristino di un'unità FIPS o SED in modalità non protetta" Per tutti i dischi all'interno della coppia ha prima dell'inizializzazione del sistema (opzioni di avvio 4 o 9). Il mancato rispetto di questa procedura potrebbe causare la perdita di dati in futuro se i dischi vengono riutilizzati.

Prima di iniziare

- È necessario conoscere l'ID della chiave di autenticazione utilizzata dal disco.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fasi

1. Assicurarsi che il disco sia stato contrassegnato come guasto:

   ```
   storage disk show -broken
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                    Usable
Physical
    Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
Size
    ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
-------
    0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
133.9GB
    0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
134.2GB
[...]
```

2. Rimuovere il disco guasto e sostituirlo con un nuovo disco FIPS o SED, seguendo le istruzioni nella guida hardware del modello di shelf di dischi in uso.
3. Assegnare la proprietà del disco appena sostituito:

   ```
   storage disk assign -disk disk_name -owner node
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   ```
   cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
   ```

4. Verificare che il nuovo disco sia stato assegnato:

   ```
   storage encryption disk show
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1   open 0x0
[...]
```

5. Assegnare le chiavi di autenticazione dei dati all'unità FIPS o SED.

   "Assegnazione di una chiave di autenticazione dei dati a un disco FIPS o SED (gestione esterna delle chiavi)"

6. Se necessario, assegnare una chiave di autenticazione FIPS 140-2 all'unità FIPS.

   "Assegnazione di una chiave di autenticazione FIPS 140-2 a un disco FIPS"

Rendere i dati su un disco FIPS o SED inaccessibili

Rendere i dati su un disco FIPS o panoramica SED inaccessibili

Se si desidera rendere i dati su un'unità FIPS o SED permanentemente inaccessibili, mantenendo lo spazio inutilizzato dell'unità disponibile per i nuovi dati, è possibile disinfettare il disco. Se si desidera rendere i dati inaccessibili in modo permanente e non è necessario riutilizzare il disco, è possibile distruggerli.

- Pulizia dei dischi

  Quando si disigienizza un'unità con crittografia automatica, il sistema modifica la chiave di crittografia del disco in un nuovo valore casuale, ripristina lo stato di blocco all'accensione su false e imposta l'ID della chiave su un valore predefinito, ovvero l'ID protetto del produttore 0x0 (unità SAS) o una chiave nulla (unità NVMe). In questo modo, i dati sul disco non sono accessibili e non possono essere recuperati. È possibile riutilizzare i dischi sanitizzati come dischi di riserva non azzerati.

- Distruggere il disco

  Quando si distrugge un disco FIPS o SED, il sistema imposta la chiave di crittografia del disco su un valore casuale sconosciuto e blocca il disco in modo irreversibile. In questo modo, il disco risulta inutilizzabile in modo permanente e i dati in esso contenuti sono inaccessibili in modo permanente.

È possibile sanificare o distruggere singole unità con crittografia automatica o tutte le unità con crittografia automatica per un nodo.

Sanificare un disco FIPS o SED

Se si desidera rendere i dati su un'unità FIPS o SED permanentemente inaccessibili e utilizzare l'unità per i nuovi dati, è possibile utilizzare `storage encryption disk sanitize` comando per la pulizia del disco.

A proposito di questa attività

Quando si disigienizza un'unità con crittografia automatica, il sistema modifica la chiave di crittografia del disco in un nuovo valore casuale, ripristina lo stato di blocco all'accensione su false e imposta l'ID della chiave su un valore predefinito, ovvero l'ID protetto del produttore 0x0 (unità SAS) o una chiave nulla (unità NVMe). In questo modo, i dati sul disco non sono accessibili e non possono essere recuperati. È possibile riutilizzare i dischi sanitizzati come dischi di riserva non azzerati.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fasi

1. Migrare tutti i dati che devono essere conservati in un aggregato su un altro disco.
2. Eliminare l'aggregato sull'unità FIPS o SED da sanificare:

   `storage aggregate delete -aggregate` *`aggregate_name`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Identificare l'ID del disco per l'unità FIPS o SED da sanificare:

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   Per la sintassi completa dei comandi, vedere la pagina man.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Se un disco FIPS è in esecuzione in modalità di conformità FIPS, impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID 0x0 predefinito:

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

È possibile utilizzare `security key-manager query` Per visualizzare gli ID chiave.

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. Igienizzare il disco:

```
storage encryption disk sanitize -disk disk_id
```

È possibile utilizzare questo comando per sanificare solo i dischi hot spare o rotti. Per sanificare tutti i dischi, indipendentemente dal tipo, utilizzare `-force-all-state` opzione. Per la sintassi completa dei comandi, vedere la pagina man.

> ONTAP richiede di inserire una frase di conferma prima di continuare. Inserire la frase esattamente come mostrato sullo schermo.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

Distruggere un disco FIPS o SED

Se si desidera rendere i dati su un'unità FIPS o SED permanentemente inaccessibili e non è necessario riutilizzarli, è possibile utilizzare `storage encryption disk destroy` comando per distruggere il disco.

A proposito di questa attività

Quando si distrugge un disco FIPS o SED, il sistema imposta la chiave di crittografia del disco su un valore casuale sconosciuto e blocca l'unità in modo irreversibile. In questo modo, il disco risulta praticamente inutilizzabile e i dati in esso contenuti permanentemente inaccessibili. Tuttavia, è possibile ripristinare le impostazioni predefinite del disco utilizzando l'ID fisico sicuro (PSID) stampato sull'etichetta del disco. Per ulteriori informazioni, vedere "Restituzione di un disco FIPS o SED in caso di smarrimento delle chiavi di autenticazione".

Non distruggere un disco FIPS o SED a meno che non si disponga del servizio non-Returnable Disk Plus (NRD Plus). La distruzione di un disco annulla la garanzia.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fasi

1. Migrare tutti i dati che devono essere conservati in un aggregato su un altro disco diverso.
2. Eliminare l'aggregato sull'unità FIPS o SED da distruggere:

   `storage aggregate delete -aggregate aggregate_name`

   Per la sintassi completa dei comandi, vedere la pagina man.

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Identificare l'ID del disco per l'unità FIPS o SED da distruggere:

   `storage encryption disk show`

   Per la sintassi completa dei comandi, vedere la pagina man.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Distruggere il disco:

   `storage encryption disk destroy -disk disk_id`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Viene richiesto di inserire una frase di conferma prima di continuare. Inserire la frase esattamente come mostrato sullo schermo.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

Dati di emergenza ridotti su un'unità FIPS o SED

In caso di emergenza di sicurezza, è possibile impedire immediatamente l'accesso a un disco FIPS o SED, anche se il sistema storage o il server KMIP non sono in grado di fornire alimentazione.

Prima di iniziare

- Se si utilizza un server KMIP privo di alimentazione, il server KMIP deve essere configurato con un elemento di autenticazione facilmente distrutto (ad esempio, una smart card o un'unità USB).
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fase

1. Eseguire la cancellazione di emergenza dei dati su un disco FIPS o SED:

Se…	Quindi…

Il sistema di storage è alimentato e hai tempo per portare il sistema di storage offline senza problemi	a. Se il sistema storage è configurato come coppia ha, disattivare il Takeover.
	b. Portare tutti gli aggregati offline ed eliminarli.
	c. Impostare il livello di privilegio su Advanced:
	`set -privilege advanced`
	d. Se il disco è in modalità di conformità FIPS, impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID predefinito:
	`storage encryption disk modify -disk * -fips-key-id 0x0`
	e. Arrestare il sistema storage.
	f. Avviare in modalità di manutenzione.
	g. Sanificare o distruggere i dischi:
	◦ Se si desidera rendere i dati sui dischi inaccessibili e continuare a riutilizzare i dischi, disinfettare i dischi:
	`disk encrypt sanitize -all`
	◦ Se si desidera rendere i dati sui dischi inaccessibili e non è necessario salvarli, distruggere i dischi:
	`disk encrypt destroy disk_id1 disk_id2 …`
		Il sistema storage è alimentato e i dati devono essere immediatamente sottratti

a. **Se si desidera rendere i dati sui dischi inaccessibili e continuare a riutilizzare i dischi, eseguire la pulizia dei dischi:**
b. Se il sistema storage è configurato come coppia ha, disattivare il Takeover.
c. Impostare il livello di privilegio su Advanced (avanzato):
`set -privilege advanced`
d. Se il disco è in modalità di conformità FIPS, impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID predefinito:
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Igienizzare il disco:
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Se si desidera rendere i dati sui dischi inaccessibili e non è necessario salvarli, distruggere i dischi:**
	b. Se il sistema storage è configurato come coppia ha, disattivare il Takeover.
	c. Impostare il livello di privilegio su Advanced (avanzato):
	`set -privilege advanced`
	d. Distruggere i dischi:
	`storage encryption disk destroy -disk * -force-all-states true`
		Il sistema di storage esegue una panoramica, lasciando il sistema in uno stato di disattivazione permanente con tutti i dati cancellati. Per utilizzare di nuovo il sistema, è necessario riconfigurarlo.

L'alimentazione è disponibile per il server KMIP ma non per il sistema storage	a. Accedere al server KMIP. b. Distruggere tutte le chiavi associate ai dischi FIPS o ai SED che contengono i dati a cui si desidera impedire l'accesso. In questo modo si impedisce l'accesso alle chiavi di crittografia del disco da parte del sistema di storage.	L'alimentazione del server KMIP o del sistema storage non è disponibile

Per la sintassi completa dei comandi, vedere le pagine man.

Restituire un'unità FIPS o SED al servizio quando le chiavi di autenticazione vengono perse

Il sistema considera un'unità FIPS o SED guasta se si perdono le chiavi di autenticazione in modo permanente e non è possibile recuperarle dal server KMIP. Sebbene non sia possibile accedere o ripristinare i dati sul disco, è possibile adottare le misure necessarie

per rendere nuovamente disponibile lo spazio inutilizzato di SED per i dati.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

A proposito di questa attività

Utilizzare questo processo solo se si è certi che le chiavi di autenticazione dell'unità FIPS o SED vengano perse in modo permanente e che non sia possibile ripristinarle.

Se i dischi sono partizionati, prima di poter avviare questo processo è necessario che siano dispartizionati.

> Il comando per dispartizionare un disco è disponibile solo a livello di DIAG e deve essere eseguito solo sotto la supervisione del supporto NetApp. **Si consiglia vivamente di contattare il supporto NetApp prima di procedere.** è inoltre possibile consultare l'articolo della Knowledge base "Come dispartizionare un disco spare in ONTAP".

Fasi

1. Restituire un'unità FIPS o SED al servizio:

Se i SEDS sono…	Seguire questa procedura…

Non in modalità di compliance FIPS o in modalità di compliance FIPS e la chiave FIPS è disponibile	a. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced` b. Reimpostare la chiave FIPS sull'ID protetto predefinito 0x0: `storage encryption disk modify -fips-key-id 0x0 -disk` *`disk_id`* c. Verificare che l'operazione sia riuscita: `storage encryption disk show-status`Se l'operazione non riesce, utilizzare la procedura PSID descritta in questo argomento. d. Sanificare il disco danneggiato: `storage encryption disk sanitize -disk` *`disk_id`*`Verificare che l'operazione sia riuscita con il comando `storage encryption disk show-status` prima di passare alla fase successiva.  e. Annullare l'esecuzione di un errore sul disco crittografato: `storage disk unfail -spare true -disk` *`disk_id`*  f. Verificare se il disco dispone di un proprietario: `storage disk show -disk` *`disk_id`*  Se il disco non dispone di un proprietario, assegnarne uno. `storage disk assign -owner node -disk` *`disk_id`*  i. Immettere il nodeshell per il nodo proprietario dei dischi che si desidera disinfettare:  `system node run -node` *`node_name`*  Eseguire `disk sanitize release` comando.  g. Uscire dalla nodeshell. Annulla errore del disco: `storage disk unfail -spare true -disk` *`disk_id`*  h. Verificare che il disco sia ora uno spare e pronto per essere riutilizzato in un aggregato: `storage disk show -disk` *`disk_id`*

In modalità di compliance FIPS, la chiave FIPS non è disponibile e i SED hanno un PSID stampato sull'etichetta	a. Ottenere il PSID del disco dall'etichetta del disco. b. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced` c. Ripristinare le impostazioni predefinite del disco: `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`*`Verificare che l'operazione sia riuscita con il comando `storage encryption disk show-status` prima di passare alla fase successiva. d. Se si utilizza ONTAP 9.8P5 o versione precedente, passare alla fase successiva. Se si esegue ONTAP 9.8P6 o versione successiva, annullare la procedura di pulizia del disco. `storage disk unfail -disk` *`disk_id`* e. Verificare se il disco dispone di un proprietario: `storage disk show -disk` *`disk_id`*  Se il disco non dispone di un proprietario, assegnarne uno. `storage disk assign -owner node -disk` *`disk_id`*  i. Immettere il nodeshell per il nodo proprietario dei dischi che si desidera disinfettare:  `system node run -node` *`node_name`*  Eseguire `disk sanitize release` comando.  f. Uscire dalla nodeshell.. Annulla errore del disco: `storage disk unfail -spare true -disk` *`disk_id`* g. Verificare che il disco sia ora uno spare e pronto per essere riutilizzato in un aggregato: `storage disk show -disk` *`disk_id`*

Per la sintassi completa dei comandi, vedere "riferimento al comando".

Consente di ripristinare un'unità FIPS o SED in modalità non protetta

Un'unità FIPS o SED è protetta da accessi non autorizzati solo se l'ID della chiave di autenticazione del nodo è impostato su un valore diverso da quello predefinito. È possibile ripristinare un'unità FIPS o SED in modalità non protetta utilizzando `storage encryption disk modify` Per impostare l'ID della chiave sul valore predefinito.

Se una coppia ha utilizza dischi SAS o NVMe con crittografia (SED, NSE, FIPS), è necessario seguire questa procedura per tutti i dischi all'interno della coppia ha prima di inizializzare il sistema (opzioni di avvio 4 o 9). Il mancato rispetto di questa procedura potrebbe causare la perdita di dati in futuro se i dischi vengono riutilizzati.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Se un disco FIPS è in esecuzione in modalità di conformità FIPS, impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID 0x0 predefinito:

   ```
   storage encryption disk modify -disk disk_id -fips-key-id 0x0
   ```

   È possibile utilizzare `security key-manager query` Per visualizzare gli ID chiave.

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   Confermare l'operazione con il comando:

   ```
   storage encryption disk show-status
   ```

   Ripetere il comando show-status fino a quando i numeri in "Disks incomincied" (dischi iniziati) e "Disks Done" (dischi eseguiti) non sono gli stessi.

   ```
   cluster1:: storage encryption disk show-status

               FIPS    Latest   Start                Execution   Disks
   Disks Disks
   Node        Support Request  Timestamp            Time (sec)  Begun
   Done  Successful
   -------     ------- -------- ------------------   ---------- ------
   ------  ----------
   cluster1    true    modify   1/18/2022 15:29:38    3           14     5
   5
   1 entry was displayed.
   ```

3. Impostare nuovamente l'ID della chiave di autenticazione dei dati per il nodo sul valore MSID 0x0 predefinito:

   ```
   storage encryption disk modify -disk disk_id -data-key-id 0x0
   ```

   Il valore di `-data-key-id` Deve essere impostato su 0x0 se si sta ripristinando un'unità SAS o NVMe in modalità non protetta.

   È possibile utilizzare `security key-manager query` Per visualizzare gli ID chiave.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

Confermare l'operazione con il comando:

```
storage encryption disk show-status
```

Ripetere il comando show-status fino a quando i numeri non coincidono. L'operazione è completa quando i numeri in "dischi iniziati" e "dischi completati" sono gli stessi.

Modalità di manutenzione

A partire da ONTAP 9.7, è possibile modificare la chiave di un disco FIPS dalla modalità di manutenzione. Utilizzare la modalità di manutenzione solo se non è possibile utilizzare le istruzioni dell'interfaccia utente di ONTAP descritte nella sezione precedente.

Fasi

1. Impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID 0x0 predefinito:

   `disk encrypt rekey_fips 0x0 *disklist*`

2. Impostare nuovamente l'ID della chiave di autenticazione dei dati per il nodo sul valore MSID 0x0 predefinito:

   `disk encrypt rekey 0x0 *disklist*`

3. Verificare che la chiave di autenticazione FIPS sia stata reinserita correttamente:

   `disk encrypt show_fips`

4. Confermare che la chiave di autenticazione dei dati è stata risigitata correttamente con:

   `disk encrypt show`

   L'output visualizza probabilmente l'ID chiave MSID 0x0 predefinito o il valore di 64 caratteri posseduto dal server delle chiavi. Il `Locked?` il campo si riferisce al blocco dei dati.

```
Disk       FIPS Key ID                 Locked?
---------- --------------------------- -------
0a.01.0    0x0                          Yes
```

Rimuovere una connessione di gestione delle chiavi esterna

È possibile scollegare un server KMIP da un nodo quando non è più necessario. Ad

esempio, è possibile scollegare un server KMIP durante la transizione alla crittografia del volume.

A proposito di questa attività

Quando si disconnette un server KMIP da un nodo in una coppia ha, il sistema disconnette automaticamente il server da tutti i nodi del cluster.

> Se si prevede di continuare a utilizzare la gestione delle chiavi esterne dopo aver scollegato un server KMIP, assicurarsi che sia disponibile un altro server KMIP per la fornitura delle chiavi di autenticazione.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

Fase

1. Disconnettere un server KMIP dal nodo corrente:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 e versioni successive	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,…`	ONTAP 9.5 e versioni precedenti

In un ambiente MetroCluster, è necessario ripetere questi comandi su entrambi i cluster per la SVM amministrativa.

Per la sintassi completa dei comandi, vedere le pagine man.

Il seguente comando ONTAP 9.6 disattiva le connessioni a due server di gestione delle chiavi esterni per `cluster1`, il primo nome `ks1`, In attesa sulla porta predefinita 5696, la seconda con l'indirizzo IP 10.0.0.20, in attesa sulla porta 24482:

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

Modificare le proprietà del server di gestione delle chiavi esterno

A partire da ONTAP 9.6, è possibile utilizzare `security key-manager external modify-server` Comando per modificare il timeout i/o e il nome utente di un server di gestione delle chiavi esterno.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- Per questa attività sono richiesti privilegi avanzati.
- In un ambiente MetroCluster, è necessario ripetere questi passaggi su entrambi i cluster per la SVM amministrativa.

Fasi

1. Sul sistema storage, passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Modificare le proprietà del server di gestione delle chiavi esterno per il cluster:

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > Il valore di timeout viene espresso in secondi. Se si modifica il nome utente, viene richiesto di inserire una nuova password. Se si esegue il comando al prompt di login del cluster, *admin_SVM* Per impostazione predefinita, viene impostata la SVM amministrativa del cluster corrente. È necessario essere l'amministratore del cluster per modificare le proprietà del server del gestore delle chiavi esterno.

   Il seguente comando modifica il valore di timeout a 45 secondi per `cluster1` server di gestione delle chiavi esterno in attesa sulla porta predefinita 5696:

   ```
   cluster1::> security key-manager external modify-server -vserver
   cluster1 -key-server ks1.local -timeout 45
   ```

3. Modificare le proprietà del server di gestione delle chiavi esterne per una SVM (solo NVE):

   ```
   security key-manager external modify-server -vserver SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > Il valore di timeout viene espresso in secondi. Se si modifica il nome utente, viene richiesto di inserire una nuova password. Se si esegue il comando al prompt di accesso SVM, *SVM* Per impostazione predefinita, viene impostata la SVM corrente. Per modificare le proprietà del server del gestore delle chiavi esterno, è necessario essere l'amministratore del cluster o SVM.

   Il seguente comando consente di modificare il nome utente e la password di `svm1` server di gestione delle chiavi esterno in attesa sulla porta predefinita 5696:

   ```
   svm1::> security key-manager external modify-server -vserver svm11 -key
   -server ks1.local -username svm1user
   Enter the password:
   Reenter the password:
   ```

4. Ripetere l'ultimo passaggio per eventuali SVM aggiuntive.

Transizione alla gestione esterna delle chiavi dalla gestione integrata delle chiavi

Se si desidera passare alla gestione esterna delle chiavi dalla gestione integrata delle chiavi, è necessario eliminare la configurazione di gestione integrata delle chiavi prima di attivare la gestione esterna delle chiavi.

Prima di iniziare

- Per la crittografia basata su hardware, è necessario ripristinare il valore predefinito delle chiavi dati di tutti i dischi FIPS o SED.

  "Ripristino di un'unità FIPS o SED in modalità non protetta"

- Per la crittografia basata su software, è necessario annullare la crittografia di tutti i volumi.

  "Annullamento della crittografia dei dati del volume"

- Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fase

1. Eliminare la configurazione di gestione delle chiavi integrata per un cluster:

Per questa versione di ONTAP…	Utilizzare questo comando…
ONTAP 9.6 e versioni successive	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 e versioni precedenti	`security key-manager delete-key-database`

Per la sintassi completa dei comandi, vedere "Pagine di manuale di ONTAP".

Transizione alla gestione delle chiavi integrata dalla gestione esterna delle chiavi

Se si desidera passare alla gestione delle chiavi integrata dalla gestione delle chiavi esterna, è necessario eliminare la configurazione di gestione delle chiavi esterne prima di poter attivare la gestione delle chiavi integrata.

Prima di iniziare

- Per la crittografia basata su hardware, è necessario ripristinare il valore predefinito delle chiavi dati di tutti i dischi FIPS o SED.

  "Ripristino di un'unità FIPS o SED in modalità non protetta"

- È necessario eliminare tutte le connessioni di gestione delle chiavi esterne.

  "Eliminazione di una connessione di gestione delle chiavi esterna"

- Per eseguire questa attività, è necessario essere un amministratore del cluster.

Procedura

I passaggi necessari per eseguire la transizione della gestione delle chiavi dipendono dalla versione di ONTAP in uso.

ONTAP 9.6 e versioni successive

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Utilizzare il comando:

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   In un ambiente MetroCluster, è necessario ripetere il comando su entrambi i cluster per la SVM amministrativa.

ONTAP 9.5 e versioni precedenti

Utilizzare il comando:
`security key-manager delete-kmip-config`

Cosa accade quando i server di gestione delle chiavi non sono raggiungibili durante il processo di avvio

ONTAP prende alcune precauzioni per evitare comportamenti indesiderati nel caso in cui un sistema storage configurato per NSE non riesca a raggiungere nessuno dei server di gestione delle chiavi specificati durante il processo di avvio.

Se il sistema di storage è configurato per NSE, i SED vengono ridigitati e bloccati e i SED sono accesi, il sistema di storage deve recuperare le chiavi di autenticazione richieste dai server di gestione delle chiavi per autenticarsi ai SED prima di poter accedere ai dati.

Il sistema storage tenta di contattare i server di gestione delle chiavi specificati per un massimo di tre ore. Se il sistema storage non riesce a raggiungerne uno dopo tale periodo, il processo di avvio si interrompe e il sistema storage si arresta.

Se il sistema di storage contatta correttamente qualsiasi server di gestione delle chiavi specificato, tenta di stabilire una connessione SSL per un massimo di 15 minuti. Se il sistema di storage non riesce a stabilire una connessione SSL con un server di gestione delle chiavi specificato, il processo di avvio si interrompe e il sistema di storage si arresta.

Mentre il sistema di storage tenta di contattare e connettersi ai server di gestione delle chiavi, visualizza informazioni dettagliate sui tentativi di contatto non riusciti alla CLI. È possibile interrompere i tentativi di contatto in qualsiasi momento premendo Ctrl-C.

Come misura di sicurezza, i SED consentono solo un numero limitato di tentativi di accesso non autorizzati, dopodiché disattivano l'accesso ai dati esistenti. Se il sistema di storage non riesce a contattare alcun server di gestione delle chiavi specificato per ottenere le chiavi di autenticazione appropriate, può solo tentare di autenticare con la chiave predefinita, il che causa un tentativo di errore e un panico. Se il sistema di storage è configurato per il riavvio automatico in caso di panico, entra in un loop di avvio che porta a tentativi di autenticazione non riusciti continui sui SED.

L'arresto del sistema storage in questi scenari è progettato per impedire al sistema storage di entrare in un loop di avvio e di perdere dati non intenzionale come conseguenza del blocco permanente dei SED dovuto al superamento del limite di sicurezza di un certo numero di tentativi di autenticazione consecutivi non riusciti. Il limite e il tipo di protezione di blocco dipendono dalle specifiche di produzione e dal tipo di SED:

TIPO SED	Numero di tentativi consecutivi di autenticazione non riusciti che hanno determinato il blocco	Tipo di protezione di blocco quando viene raggiunto il limite di sicurezza
DISCO RIGIDO	1024	Permanente. I dati non possono essere recuperati, anche quando la chiave di autenticazione appropriata diventa nuovamente disponibile.
X440_PHM2800 MCTO SSD NSE da 800 GB con revisioni del firmware NA00 o NA01	5	Temporaneo. Il blocco è valido solo fino a quando il disco non viene spento e riacceso.
X577_PHM2800 MCTO SSD NSE da 800 GB con revisioni del firmware NA00 o NA01	5	Temporaneo. Il blocco è valido solo fino a quando il disco non viene spento e riacceso.
X440_PHM2800MCTO SSD NSE da 800 GB con revisioni del firmware superiori	1024	Permanente. I dati non possono essere recuperati, anche quando la chiave di autenticazione appropriata diventa nuovamente disponibile.
X577_PHM2800MCTO SSD NSE da 800 GB con revisioni del firmware superiori	1024	Permanente. I dati non possono essere recuperati, anche quando la chiave di autenticazione appropriata diventa nuovamente disponibile.
Tutti gli altri modelli di SSD	1024	Permanente. I dati non possono essere recuperati, anche quando la chiave di autenticazione appropriata diventa nuovamente disponibile.

Per tutti i tipi SED, un'autenticazione corretta azzera il numero di proy.

Se si verifica questo scenario in cui il sistema storage viene arrestato a causa di un errore di accesso a uno dei server di gestione delle chiavi specificati, prima di continuare l'avvio del sistema storage è necessario identificare e correggere la causa dell'errore di comunicazione.

Disattivare la crittografia per impostazione predefinita

A partire da ONTAP 9.7, la crittografia aggregata e del volume è attivata per impostazione predefinita se si dispone di una licenza di crittografia del volume (VE) e si utilizza un gestore di chiavi integrato o esterno. Se necessario, è possibile disattivare la crittografia per impostazione predefinita per l'intero cluster.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o un amministratore SVM al quale l'amministratore del cluster ha delegato l'autorità.

Fase

1. Per disattivare la crittografia per impostazione predefinita per l'intero cluster in ONTAP 9.7 o versioni successive, eseguire il seguente comando:

   ```
   options -option-name encryption.data_at_rest_encryption.disable_by_default
   -option-value on
   ```