



Configurare le impostazioni del cluster

Element Software

NetApp

November 12, 2025

This PDF was generated from https://docs.netapp.com/it-it/element-software-128/storage/task_system_manage_cluster_enable_and_disable_encryption_for_a_cluster.html on November 12, 2025. Always check docs.netapp.com for the latest.

Sommario

Configurare le impostazioni del cluster	1
Abilitare e disabilitare la crittografia a riposo per un cluster	1
Controllare lo stato di crittografia a riposo	1
Abilita la crittografia basata su hardware a riposo	1
Abilita la crittografia basata su software a riposo	2
Disabilitare la crittografia basata su hardware a riposo	2
Imposta la soglia di riempimento del cluster	2
Trova maggiori informazioni	2
Abilita e disabilita il bilanciamento del carico del volume	2
Trova maggiori informazioni	3
Abilita e disabilita l'accesso al supporto	3
Gestisci il banner Termini di utilizzo	3
Abilita il banner Termini di utilizzo	3
Modifica il banner dei Termini di utilizzo	4
Disattiva il banner Termini di utilizzo	4
Imposta il protocollo di tempo di rete	4
Configurare i server Network Time Protocol affinché il cluster esegua le query	4
Configurare il cluster per ascoltare le trasmissioni NTP	5
Gestisci SNMP	6
Scopri di più su SNMP	6
Configurare un richiedente SNMP	6
Configurare un utente USM SNMP	7
Configurare le trappole SNMP	7
Visualizzare i dati degli oggetti gestiti utilizzando i file della base di informazioni di gestione	8
Gestisci unità	8
Dettagli delle unità	8
Per maggiori informazioni	9
Gestisci nodi	9
Gestisci nodi	9
Aggiungere un nodo a un cluster	10
Versionamento e compatibilità dei nodi	11
Capacità del cluster in un ambiente di nodi misti	11
Visualizza i dettagli del nodo	12
Visualizza i dettagli delle porte Fibre Channel	13
Trova maggiori informazioni	14
Gestire reti virtuali	14
Gestire reti virtuali	14
Aggiungi una rete virtuale	14
Abilita il routing e l'inoltro virtuali	15
Modifica una rete virtuale	16
Modifica VLAN VRF	16
Elimina una rete virtuale	17

Configurare le impostazioni del cluster

Abilitare e disabilitare la crittografia a riposo per un cluster

Con i cluster SolidFire è possibile crittografare tutti i dati inattivi archiviati sulle unità del cluster. È possibile abilitare la protezione a livello di cluster delle unità auto-crittografanti (SED) utilizzando ["crittografia a riposo basata su hardware o software"](#).

È possibile abilitare la crittografia hardware a riposo tramite l'interfaccia utente o l'API di Element. L'abilitazione della funzionalità di crittografia hardware a riposo non influisce sulle prestazioni o sull'efficienza del cluster. È possibile abilitare la crittografia software a riposo solo tramite l'API Element.

La crittografia basata su hardware a riposo non è abilitata per impostazione predefinita durante la creazione del cluster e può essere abilitata e disabilitata dall'interfaccia utente di Element.



Per i cluster di archiviazione all-flash SolidFire, la crittografia software a riposo deve essere abilitata durante la creazione del cluster e non può essere disabilitata dopo la creazione del cluster.

Cosa ti servirà

- Si dispone dei privilegi di amministratore del cluster per abilitare o modificare le impostazioni di crittografia.
- Per la crittografia a riposo basata su hardware, è necessario assicurarsi che il cluster sia in uno stato di integrità prima di modificare le impostazioni di crittografia.
- Se si disabilita la crittografia, è necessario che due nodi partecipino a un cluster per accedere alla chiave per disabilitare la crittografia su un'unità.

Controllare lo stato di crittografia a riposo

Per visualizzare lo stato corrente della crittografia a riposo e/o della crittografia software a riposo sul cluster, utilizzare ["Ottieni informazioni sul cluster"](#) metodo. Puoi usare il ["Ottieni informazioni sulla crittografia software a riposo"](#) metodo per ottenere le informazioni che il cluster utilizza per crittografare i dati a riposo.



La dashboard dell'interfaccia utente del software Element su <https://<MVIP>/> attualmente mostra solo lo stato di crittografia a riposo per la crittografia basata su hardware.

Opzioni

- [Abilita la crittografia basata su hardware a riposo](#)
- [Abilita la crittografia basata su software a riposo](#)
- [Disabilitare la crittografia basata su hardware a riposo](#)

Abilita la crittografia basata su hardware a riposo



Per abilitare la crittografia a riposo utilizzando una configurazione di gestione delle chiavi esterna, è necessario abilitare la crittografia a riposo tramite ["API"](#). L'abilitazione tramite il pulsante Element UI esistente ripristinerà l'utilizzo delle chiavi generate internamente.

1. Dall'interfaccia utente dell'elemento, seleziona **Cluster > Impostazioni**.

2. Selezionare **Abilita crittografia a riposo**.

Abilita la crittografia basata su software a riposo



La crittografia software a riposo non può essere disabilitata dopo essere stata abilitata sul cluster.

1. Durante la creazione del cluster, eseguire il comando "[metodo di creazione del cluster](#)" con `enableSoftwareEncryptionAtRest` impostato su `true`.

Disabilitare la crittografia basata su hardware a riposo

1. Dall'interfaccia utente dell'elemento, seleziona **Cluster > Impostazioni**.
2. Selezionare **Disabilita crittografia a riposo**.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Imposta la soglia di riempimento del cluster

È possibile modificare il livello al quale il sistema genera un avviso di riempimento del cluster di blocchi seguendo i passaggi indicati di seguito. Inoltre, è possibile utilizzare il metodo API `ModifyClusterFullThreshold` per modificare il livello in cui il sistema genera un avviso di blocco o di metadati.

Cosa ti servirà

È necessario disporre dei privilegi di amministratore del cluster.

Passi

1. Fare clic su **Cluster > Impostazioni**.
2. Nella sezione Impostazioni complete del cluster, immettere una percentuale in **Genera un avviso quando rimane _% di capacità prima che Helix non riesca a riprendersi da un errore del nodo**.
3. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

["Come vengono calcolate le soglie di blockSpace per Element"](#)

Abilita e disabilita il bilanciamento del carico del volume

A partire da Element 12.8, è possibile utilizzare Volume Load Balancing per bilanciare i volumi tra i nodi in base agli IOPS effettivi di ciascun volume anziché agli IOPS minimi configurati nella policy QoS. È possibile abilitare e disabilitare il bilanciamento del carico del volume, disabilitato per impostazione predefinita, tramite l'interfaccia utente o l'API di Element.

Passi

1. Selezionare **Cluster > Impostazioni**.
2. Nella sezione Cluster Specific, modifica lo stato per Volume Load Balancing:

Abilita il bilanciamento del carico del volume

Selezionare **Abilita bilanciamento del carico su IOPS effettivi** e confermare la selezione.

Disabilita il bilanciamento del carico del volume:

Selezionare **Disabilita bilanciamento del carico su IOPS effettivi** e confermare la selezione.

3. Facoltativamente, selezionare **Reporting > Panoramica** per confermare la modifica dello stato per il saldo sugli IOPS effettivi. Potrebbe essere necessario scorrere verso il basso le informazioni sullo stato del cluster per visualizzarne lo stato.

Trova maggiori informazioni

- ["Abilita il bilanciamento del carico del volume tramite l'API"](#)
- ["Disabilitare il bilanciamento del carico del volume tramite l'API"](#)
- ["Creare e gestire policy QoS del volume"](#)

Abilita e disabilita l'accesso al supporto

È possibile abilitare l'accesso al supporto per consentire temporaneamente al personale di supporto NetApp di accedere ai nodi di storage tramite SSH per la risoluzione dei problemi.

Per modificare l'accesso al supporto è necessario disporre dei privilegi di amministratore del cluster.

1. Fare clic su **Cluster > Impostazioni**.
2. Nella sezione Abilita/Disabilita accesso supporto, inserisci la durata (in ore) per cui desideri consentire l'accesso al supporto.
3. Fare clic su **Abilita accesso supporto**.
4. **Facoltativo:** per disattivare l'accesso al supporto, fare clic su **Disattiva accesso al supporto**.

Gestisci il banner Termini di utilizzo

È possibile abilitare, modificare o configurare un banner contenente un messaggio per l'utente.

Opzioni

[Abilita il banner Termini di utilizzo](#) [Modifica il banner dei Termini di utilizzo](#) [Disattiva il banner Termini di utilizzo](#)

Abilita il banner Termini di utilizzo

È possibile abilitare un banner con i Termini di utilizzo che viene visualizzato quando un utente accede all'interfaccia utente di Element. Quando l'utente clicca sul banner, viene visualizzata una finestra di dialogo di

testo contenente il messaggio configurato per il cluster. Il banner può essere rimosso in qualsiasi momento.

Per abilitare la funzionalità Termini di utilizzo è necessario disporre dei privilegi di amministratore del cluster.

1. Fare clic su **Utenti > Termini di utilizzo**.
2. Nel modulo **Termini di utilizzo**, immettere il testo da visualizzare nella finestra di dialogo Termini di utilizzo.



Non superare i 4096 caratteri.

3. Fare clic su **Abilita**.

Modifica il banner dei Termini di utilizzo

Puoi modificare il testo che un utente vede quando seleziona il banner di accesso ai Termini di utilizzo.

Cosa ti servirà

- Per configurare i Termini di utilizzo è necessario disporre dei privilegi di amministratore del cluster.
- Assicurati che la funzione Termini di utilizzo sia abilitata.

Passi

1. Fare clic su **Utenti > Termini di utilizzo**.
2. Nella finestra di dialogo **Termini di utilizzo**, modifica il testo che desideri visualizzare.



Non superare i 4096 caratteri.

3. Fare clic su **Salva modifiche**.

Disattiva il banner Termini di utilizzo

Puoi disattivare il banner Termini di utilizzo. Con il banner disabilitato, all'utente non viene più richiesto di accettare i termini di utilizzo quando utilizza Element UI.

Cosa ti servirà

- Per configurare i Termini di utilizzo è necessario disporre dei privilegi di amministratore del cluster.
- Assicurati che i Termini di utilizzo siano abilitati.

Passi

1. Fare clic su **Utenti > Termini di utilizzo**.
2. Fare clic su **Disabilita**.

Imposta il protocollo di tempo di rete

Configurare i server Network Time Protocol affinché il cluster esegua le query

È possibile istruire ciascun nodo di un cluster a interrogare un server NTP (Network Time Protocol) per gli aggiornamenti. Il cluster contatta solo i server configurati e richiede loro informazioni NTP.

L'NTP viene utilizzato per sincronizzare gli orologi su una rete. La connessione a un server NTP interno o esterno dovrebbe essere parte della configurazione iniziale del cluster.

Configurare NTP sul cluster in modo che punti a un server NTP locale. È possibile utilizzare l'indirizzo IP o il nome host FQDN. Il server NTP predefinito al momento della creazione del cluster è impostato su `us.pool.ntp.org`; tuttavia, a seconda della posizione fisica del cluster SolidFire, non è sempre possibile stabilire una connessione a questo sito.

L'utilizzo dell'FQDN dipende dal fatto che le impostazioni DNS del singolo nodo di archiviazione siano corrette e operative. Per farlo, configura i server DNS su ogni nodo di archiviazione e assicurati che le porte siano aperte consultando la pagina [Requisiti delle porte di rete](#).

È possibile inserire fino a cinque server NTP diversi.



È possibile utilizzare sia indirizzi IPv4 che IPv6.

Cosa ti servirà

Per configurare questa impostazione è necessario disporre dei privilegi di amministratore del cluster.

Passi

1. Configurare un elenco di IP e/o FQDN nelle impostazioni del server.
2. Assicurarsi che il DNS sia impostato correttamente sui nodi.
3. Fare clic su **Cluster > Impostazioni**.
4. In Impostazioni Network Time Protocol, seleziona **No**, che utilizza la configurazione NTP standard.
5. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

- ["Configurare il cluster per ascoltare le trasmissioni NTP"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Configurare il cluster per ascoltare le trasmissioni NTP

Utilizzando la modalità broadcast, è possibile istruire ciascun nodo di un cluster ad ascoltare sulla rete i messaggi broadcast NTP (Network Time Protocol) provenienti da un server specifico.

L'NTP viene utilizzato per sincronizzare gli orologi su una rete. La connessione a un server NTP interno o esterno dovrebbe essere parte della configurazione iniziale del cluster.

Cosa ti servirà

- Per configurare questa impostazione è necessario disporre dei privilegi di amministratore del cluster.
- È necessario configurare un server NTP sulla rete come server broadcast.

Passi

1. Fare clic su **Cluster > Impostazioni**.
2. Inserire nell'elenco dei server il server o i server NTP che utilizzano la modalità broadcast.

3. In Impostazioni Network Time Protocol, seleziona **Sì** per utilizzare un client broadcast.
4. Per impostare il client broadcast, nel campo **Server**, immettere il server NTP configurato in modalità broadcast.
5. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

- ["Configurare i server Network Time Protocol affinché il cluster esegua le query"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Gestisci SNMP

Scopri di più su SNMP

È possibile configurare il protocollo SNMP (Simple Network Management Protocol) nel cluster.

È possibile selezionare un richiedente SNMP, selezionare la versione di SNMP da utilizzare, identificare l'utente USM (User-based Security Model) SNMP e configurare trap per monitorare il cluster SolidFire . È inoltre possibile visualizzare e accedere ai file della base dati di gestione.



È possibile utilizzare sia indirizzi IPv4 che IPv6.

Dettagli SNMP

Nella pagina SNMP della scheda Cluster è possibile visualizzare le seguenti informazioni.

- **MIB SNMP**

I file MIB disponibili per la visualizzazione o il download.

- **Impostazioni SNMP generali**

È possibile abilitare o disabilitare SNMP. Dopo aver abilitato SNMP, puoi scegliere quale versione utilizzare. Se si utilizza la versione 2, è possibile aggiungere richiedenti, mentre se si utilizza la versione 3, è possibile impostare utenti USM.

- **Impostazioni trap SNMP**

Puoi identificare le trappole che vuoi catturare. È possibile impostare l'host, la porta e la stringa della community per ciascun destinatario della trap.

Configurare un richiedente SNMP

Quando è abilitata la versione 2 di SNMP, è possibile abilitare o disabilitare un richiedente e configurare i richiedenti per ricevere richieste SNMP autorizzate.

1. Fare clic sul **Cluster** > **SNMP**.

2. In **Impostazioni SNMP generali**, fare clic su **Sì** per abilitare SNMP.
3. Dall'elenco **Versione**, seleziona **Versione 2**.
4. Nella sezione **Richiedenti**, immettere le informazioni **Stringa della community** e **Rete**.



Per impostazione predefinita, la stringa della community è public e la rete è localhost. È possibile modificare queste impostazioni predefinite.

5. **Facoltativo:** per aggiungere un altro richiedente, fare clic su **Aggiungi un richiedente** e immettere le informazioni **Stringa della community** e **Rete**.
6. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

- [Configurare le trappole SNMP](#)
- [Visualizzare i dati degli oggetti gestiti utilizzando i file della base di informazioni di gestione](#)

Configurare un utente USM SNMP

Quando si abilita SNMP versione 3, è necessario configurare un utente USM per ricevere richieste SNMP autorizzate.

1. Fare clic su **Cluster > SNMP**.
2. In **Impostazioni SNMP generali**, fare clic su **Sì** per abilitare SNMP.
3. Dall'elenco **Versione**, seleziona **Versione 3**.
4. Nella sezione **Utenti USM**, immettere il nome, la password e la passphrase.
5. **Facoltativo:** per aggiungere un altro utente USM, fare clic su **Aggiungi un utente USM** e immettere nome, password e passphrase.
6. Fare clic su **Salva modifiche**.

Configurare le trappole SNMP

Gli amministratori di sistema possono utilizzare trap SNMP, note anche come notifiche, per monitorare lo stato di salute del cluster SolidFire .

Quando le trap SNMP sono abilitate, il cluster SolidFire genera trap associate alle voci del registro eventi e agli avvisi di sistema. Per ricevere le notifiche SNMP, è necessario scegliere le trappole da generare e identificare i destinatari delle informazioni sulle trappole. Per impostazione predefinita, non vengono generate trappole.

1. Fare clic su **Cluster > SNMP**.
2. Selezionare uno o più tipi di trap nella sezione **Impostazioni trap SNMP** che il sistema deve generare:
 - Cluster Fault Traps
 - Cluster Resolved Fault Traps
 - Trappole per eventi cluster
3. Nella sezione **Destinatari trap**, immettere le informazioni relative all'host, alla porta e alla stringa di community per un destinatario.

4. **Facoltativo:** per aggiungere un altro destinatario della trappola, fare clic su **Aggiungi un destinatario della trappola** e immettere le informazioni relative a host, porta e stringa della community.
5. Fare clic su **Salva modifiche**.

Visualizzare i dati degli oggetti gestiti utilizzando i file della base di informazioni di gestione

È possibile visualizzare e scaricare i file MIB (Management Information Base) utilizzati per definire ciascuno degli oggetti gestiti. La funzionalità SNMP supporta l'accesso in sola lettura agli oggetti definiti in SolidFire-StorageCluster-MIB.

I dati statistici forniti nel MIB mostrano l'attività del sistema per quanto segue:

- Statistiche del cluster
- Statistiche di volume
- Volumi per statistiche di conto
- Statistiche del nodo
- Altri dati come report, errori ed eventi di sistema

Il sistema supporta anche l'accesso al file MIB contenente i punti di accesso di livello superiore (OIDs) ai prodotti della serie SF.

Passi

1. Fare clic su **Cluster > SNMP**.
2. In **SNMP MIB**, fare clic sul file MIB che si desidera scaricare.
3. Nella finestra di download visualizzata, apri o salva il file MIB.

Gestisci unità

Ogni nodo contiene una o più unità fisiche utilizzate per archiviare una parte dei dati del cluster. Il cluster utilizza la capacità e le prestazioni dell'unità dopo che questa è stata aggiunta correttamente a un cluster. È possibile utilizzare l'interfaccia utente di Element per gestire le unità.

Dettagli delle unità

La pagina Unità nella scheda Cluster fornisce un elenco delle unità attive nel cluster. È possibile filtrare la pagina selezionando tra le schede Attivo, Disponibile, Rimozione, Cancellazione e Non riuscito.

Quando si inizializza per la prima volta un cluster, l'elenco delle unità attive è vuoto. È possibile aggiungere unità non assegnate a un cluster ed elencate nella scheda Disponibili dopo la creazione di un nuovo cluster SolidFire .

Nell'elenco delle unità attive compaiono i seguenti elementi.

- **ID unità**

Numero sequenziale assegnato all'unità.

- **ID nodo**

Numero di nodo assegnato quando il nodo viene aggiunto al cluster.

- **Nome nodo**

Il nome del nodo che ospita l'unità.

- **Fessura**

Il numero dello slot in cui si trova fisicamente l'unità.

- **Capacità**

La dimensione dell'unità, in GB.

- **Seriale**

Il numero di serie dell'unità.

- **Usura rimanente**

L'indicatore del livello di usura.

Il sistema di archiviazione segnala la quantità approssimativa di usura disponibile su ciascuna unità a stato solido (SSD) per la scrittura e la cancellazione dei dati. Un'unità che ha consumato il 5 percento dei cicli di scrittura e cancellazione previsti segnala un'usura residua del 95 percento. Il sistema non aggiorna automaticamente le informazioni sull'usura dell'unità; è possibile aggiornare o chiudere e ricaricare la pagina per aggiornare le informazioni.

- **Tipo**

Il tipo di unità. Il tipo può essere blocco o metadati.

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Gestisci nodi

Gestisci nodi

È possibile gestire lo storage SolidFire e i nodi Fibre Channel dalla pagina Nodi della scheda Cluster.

Se un nodo appena aggiunto rappresenta più del 50 percento della capacità totale del cluster, parte della capacità di questo nodo viene resa inutilizzabile ("bloccata"), in modo da rispettare la regola sulla capacità. Questa situazione rimane invariata finché non viene aggiunto altro spazio di archiviazione. Se viene aggiunto un nodo molto grande che non rispetta la regola della capacità, il nodo precedentemente bloccato non sarà più bloccato, mentre il nodo appena aggiunto diventerà bloccato. Per evitare che ciò accada, la capacità dovrebbe essere sempre aggiunta in coppia. Quando un nodo si blocca, viene generato un errore di cluster appropriato.

Aggiungere un nodo a un cluster

È possibile aggiungere nodi a un cluster quando è necessario più spazio di archiviazione o dopo la creazione del cluster. I nodi richiedono una configurazione iniziale quando vengono accesi per la prima volta. Dopo aver configurato il nodo, questo viene visualizzato nell'elenco dei nodi in sospeso ed è possibile aggiungerlo a un cluster.

La versione del software su ciascun nodo di un cluster deve essere compatibile. Quando si aggiunge un nodo a un cluster, il cluster installa la versione cluster del software NetApp Element sul nuovo nodo, secondo necessità.

È possibile aggiungere nodi di capacità più piccole o più grandi a un cluster esistente. È possibile aggiungere capacità di nodi maggiori a un cluster per consentire la crescita della capacità. I nodi più grandi aggiunti a un cluster con nodi più piccoli devono essere aggiunti a coppie. Ciò consente a Double Helix di disporre di spazio sufficiente per spostare i dati nel caso in cui uno dei nodi più grandi dovesse guastarsi. È possibile aggiungere capacità di nodi più piccole a un cluster di nodi più grande per migliorare le prestazioni.



Se un nodo appena aggiunto rappresenta più del 50 percento della capacità totale del cluster, parte della capacità di questo nodo viene resa inutilizzabile ("bloccata"), in modo da rispettare la regola sulla capacità. Questa situazione rimane invariata finché non viene aggiunto altro spazio di archiviazione. Se viene aggiunto un nodo molto grande che non rispetta la regola della capacità, il nodo precedentemente bloccato non sarà più bloccato, mentre il nodo appena aggiunto diventerà bloccato. Per evitare che ciò accada, la capacità dovrebbe essere sempre aggiunta in coppia. Quando un nodo diventa inutilizzabile, viene generato l'errore cluster strandedCapacity.

["Video NetApp : Scalabilità in base alle tue esigenze: espansione di un cluster SolidFire"](#)

È possibile aggiungere nodi agli appliance NetApp HCI .

Passi

1. Selezionare **Cluster > Nodi**.
2. Fare clic su **In attesa** per visualizzare l'elenco dei nodi in attesa.

Una volta completato il processo di aggiunta dei nodi, questi vengono visualizzati nell'elenco Nodi attivi. Fino ad allora, i nodi in sospeso vengono visualizzati nell'elenco Attivi in sospeso.

SolidFire installa la versione software Element del cluster sui nodi in sospeso quando li aggiungi a un cluster. Potrebbero volerci alcuni minuti.

3. Eseguire una delle seguenti operazioni:
 - Per aggiungere singoli nodi, fare clic sull'icona **Azioni** relativa al nodo che si desidera aggiungere.
 - Per aggiungere più nodi, seleziona la casella di controllo dei nodi da aggiungere, quindi **Azioni in blocco**. **Nota:** se il nodo che stai aggiungendo ha una versione del software Element diversa da quella in esecuzione sul cluster, il cluster aggiorna in modo asincrono il nodo alla versione del software Element in esecuzione sul master del cluster. Dopo l'aggiornamento, il nodo si aggiunge automaticamente al cluster. Durante questo processo asincrono, il nodo sarà nello stato pendingActive.

4. Fare clic su **Aggiungi**.

Il nodo appare nell'elenco dei nodi attivi.

Trova maggiori informazioni

[Versionamento e compatibilità dei nodi](#)

Versionamento e compatibilità dei nodi

La compatibilità dei nodi si basa sulla versione del software Element installata su un nodo. I cluster di storage basati sul software Element creano automaticamente un'immagine di un nodo nella versione del software Element sul cluster se il nodo e il cluster non hanno versioni compatibili.

L'elenco seguente descrive i livelli di significatività della versione software che compongono il numero di versione del software Element:

- **Maggiore**

Il primo numero indica la versione del software. Un nodo con un numero di componente principale non può essere aggiunto a un cluster contenente nodi con un numero di patch principale diverso, né è possibile creare un cluster con nodi con versioni principali miste.

- **Minore**

Il secondo numero indica funzionalità software minori o miglioramenti alle funzionalità software esistenti che sono stati aggiunti a una versione principale. Questo componente viene incrementato all'interno di un componente di versione principale per indicare che questa versione incrementale non è compatibile con nessun'altra versione incrementale del software Element con un componente secondario diverso. Ad esempio, 11.0 non è compatibile con 11.1 e 11.1 non è compatibile con 11.2.

- **Micro**

Il terzo numero indica una patch compatibile (release incrementale) con la versione del software Element rappresentata dai componenti major.minor. Ad esempio, 11.0.1 è compatibile con 11.0.2 e 11.0.2 è compatibile con 11.0.3.

Per garantire la compatibilità, i numeri di versione principale e secondaria devono corrispondere. Per garantire la compatibilità, i micronumeri non devono necessariamente corrispondere.

Capacità del cluster in un ambiente di nodi misti

È possibile combinare diversi tipi di nodi in un cluster. Le serie SF 2405, 3010, 4805, 6010, 9605, 9010, 19210, 38410 e la serie H possono coesistere in un cluster.

La serie H è composta dai nodi H610S-1, H610S-2, H610S-4 e H410S. Questi nodi supportano sia 10GbE che 25GbE.

È meglio non mescolare nodi crittografati e non crittografati. In un cluster con nodi misti, nessun nodo può essere più grande del 33 per cento della capacità totale del cluster. Ad esempio, in un cluster con quattro nodi SF-Series 4805, il nodo più grande che può essere aggiunto da solo è un SF-Series 9605. La soglia di

capacità del cluster viene calcolata in base alla potenziale perdita del nodo più grande in questa situazione.

A seconda della versione del software Element, i seguenti nodi di archiviazione della serie SF non sono supportati:

A partire da...	Nodo di archiviazione non supportato...
Elemento 12.8	<ul style="list-style-type: none">• SF4805• SF9605• SF19210• SF38410
Elemento 12.7	<ul style="list-style-type: none">• SF2405• SF9608
Elemento 12.0	<ul style="list-style-type: none">• SF3010• SF6010• SF9010

Se si tenta di aggiornare uno di questi nodi a una versione di Element non supportata, verrà visualizzato un errore che indica che il nodo non è supportato da Element 12.x.

Visualizza i dettagli del nodo

È possibile visualizzare i dettagli dei singoli nodi, ad esempio tag di servizio, dettagli dell'unità e grafici per l'utilizzo e statistiche dell'unità. La pagina Nodi della scheda Cluster fornisce la colonna Versione in cui è possibile visualizzare la versione software di ciascun nodo.

Passi

1. Fare clic su **Cluster > Nodi**.
2. Per visualizzare i dettagli di un nodo specifico, fare clic sull'icona **Azioni** per un nodo.
3. Fare clic su **Visualizza dettagli**.
4. Esaminare i dettagli del nodo:
 - **ID nodo**: ID generato dal sistema per il nodo.
 - **Nome nodo**: il nome host del nodo.
 - **Ruolo del nodo**: il ruolo che il nodo ha nel cluster. Valori possibili:
 - Cluster Master: il nodo che esegue attività amministrative a livello di cluster e contiene MVIP e SVIP.
 - Nodo ensemble: un nodo che partecipa al cluster. A seconda della dimensione del cluster, sono presenti 3 o 5 nodi ensemble.
 - Fibre Channel: un nodo del cluster.
 - **Tipo di nodo**: il tipo di modello del nodo.

- **Unità attive:** numero di unità attive nel nodo.
- **Utilizzo del nodo:** percentuale di utilizzo del nodo in base a nodeHeat. Il valore visualizzato è recentPrimaryTotalHeat in percentuale. Disponibile a partire da Element 12.8.
- **IP di gestione:** indirizzo IP di gestione (MIP) assegnato al nodo per le attività di amministrazione di rete da 1 GbE o 10 GbE.
- **IP del cluster:** l'indirizzo IP del cluster (CIP) assegnato al nodo utilizzato per la comunicazione tra i nodi nello stesso cluster.
- **IP di archiviazione:** l'indirizzo IP di archiviazione (SIP) assegnato al nodo utilizzato per la scoperta della rete iSCSI e per tutto il traffico dati della rete.
- **ID VLAN di gestione:** ID virtuale per la rete locale di gestione.
- **ID VLAN di archiviazione:** ID virtuale per la rete locale di archiviazione.
- **Versione:** la versione del software in esecuzione su ciascun nodo.
- **Porta di replicazione:** la porta utilizzata sui nodi per la replica remota.
- **Tag di servizio:** il numero univoco del tag di servizio assegnato al nodo.
- **Dominio di protezione personalizzato:** il dominio di protezione personalizzato assegnato al nodo.

Visualizza i dettagli delle porte Fibre Channel

È possibile visualizzare i dettagli delle porte Fibre Channel, come lo stato, il nome e l'indirizzo della porta, dalla pagina Porte FC.

Visualizza le informazioni sulle porte Fibre Channel connesse al cluster.

Passi

1. Fare clic su **Cluster > Porte FC**.
2. Per filtrare le informazioni in questa pagina, clicca su **Filtra**.
3. Esamina i dettagli:
 - **ID nodo:** il nodo che ospita la sessione per la connessione.
 - **Nome nodo:** Nome del nodo generato dal sistema.
 - **Slot:** Numero dello slot in cui si trova la porta Fibre Channel.
 - **Porta HBA:** porta fisica sull'adattatore bus host (HBA) Fibre Channel.
 - **WWNN:** Nome del nodo mondiale.
 - **WWPN:** Nome della porta mondiale di destinazione.
 - **Switch WWN:** Nome mondiale dello switch Fibre Channel.
 - **Stato del porto:** Stato attuale del porto.
 - **nPort ID:** ID della porta del nodo sulla struttura Fibre Channel.
 - **Velocità:** la velocità Fibre Channel negoziata. I valori possibili sono i seguenti:
 - 4Gbps
 - 8Gbps
 - 16Gbps

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Gestire reti virtuali

Gestire reti virtuali

La rete virtuale nello storage SolidFire consente di connettere a un unico cluster il traffico tra più client che si trovano su reti logiche separate. Le connessioni al cluster sono separate nello stack di rete tramite l'uso del tagging VLAN.

Trova maggiori informazioni

- [Aggiungi una rete virtuale](#)
- [Abilita il routing e l'inoltro virtuali](#)
- [Modifica una rete virtuale](#)
- [Modifica VLAN VRF](#)
- [Elimina una rete virtuale](#)

Aggiungi una rete virtuale

È possibile aggiungere una nuova rete virtuale a una configurazione cluster per abilitare una connessione di ambiente multi-tenant a un cluster che esegue il software Element.

Cosa ti servirà

- Identificare il blocco di indirizzi IP che verrà assegnato alle reti virtuali sui nodi del cluster.
- Identificare un indirizzo IP di rete di storage (SVIP) che verrà utilizzato come endpoint per tutto il traffico di storage NetApp Element .



Per questa configurazione è necessario considerare i seguenti criteri:

- Le VLAN che non sono abilitate per VRF richiedono che gli iniziatori si trovino nella stessa subnet dell'SVIP.
- Le VLAN abilitate per VRF non richiedono che gli iniziatori si trovino nella stessa subnet dell'SVIP e il routing è supportato.
- L'SVIP predefinito non richiede che gli iniziatori si trovino nella stessa subnet dell'SVIP e il routing è supportato.

Quando si aggiunge una rete virtuale, viene creata un'interfaccia per ciascun nodo e ciascuno richiede un indirizzo IP di rete virtuale. Il numero di indirizzi IP specificato durante la creazione di una nuova rete virtuale deve essere uguale o maggiore del numero di nodi nel cluster. Gli indirizzi di rete virtuale vengono forniti in blocco e assegnati automaticamente ai singoli nodi. Non è necessario assegnare manualmente gli indirizzi di rete virtuale ai nodi del cluster.

Passi

1. Fare clic su **Cluster > Rete**.
2. Fare clic su **Crea VLAN**.
3. Nella finestra di dialogo **Crea una nuova VLAN**, immettere i valori nei seguenti campi:
 - **Nome VLAN**
 - **Tag VLAN**
 - **SVIP**
 - **Maschera di rete**
 - (Facoltativo) **Descrizione**
4. Immettere l'indirizzo **IP iniziale** per l'intervallo di indirizzi IP in **Blocchi di indirizzi IP**.
5. Immettere la **Dimensione** dell'intervallo IP come numero di indirizzi IP da includere nel blocco.
6. Fare clic su **Aggiungi un blocco** per aggiungere un blocco non continuo di indirizzi IP per questa VLAN.
7. Fare clic su **Crea VLAN**.

Visualizza i dettagli della rete virtuale

Passi

1. Fare clic su **Cluster > Rete**.
2. Esamina i dettagli.
 - **ID**: ID univoco della rete VLAN, assegnato dal sistema.
 - **Nome**: Nome univoco assegnato dall'utente per la rete VLAN.
 - **Tag VLAN**: tag VLAN assegnato al momento della creazione della rete virtuale.
 - **SVIP**: Indirizzo IP virtuale di archiviazione assegnato alla rete virtuale.
 - **Netmask**: Maschera di rete per questa rete virtuale.
 - **Gateway**: Indirizzo IP univoco di un gateway di rete virtuale. VRF deve essere abilitato.
 - **VRF abilitato**: Indica se il routing e l'inoltro virtuali sono abilitati o meno.
 - **IP utilizzati**: intervallo di indirizzi IP di rete virtuale utilizzati per la rete virtuale.

Abilita il routing e l'inoltro virtuali

È possibile abilitare il routing e l'inoltro virtuali (VRF), che consente a più istanze di una tabella di routing di esistere in un router e di funzionare simultaneamente. Questa funzionalità è disponibile solo per le reti di archiviazione.

È possibile abilitare VRF solo al momento della creazione di una VLAN. Se si desidera tornare a non-VRF, è necessario eliminare e ricreare la VLAN.

1. Fare clic su **Cluster > Rete**.
2. Per abilitare VRF su una nuova VLAN, selezionare **Crea VLAN**.
 - a. Inserire le informazioni rilevanti per il nuovo VRF/VLAN. Vedere Aggiunta di una rete virtuale.
 - b. Selezionare la casella di controllo **Abilita VRF**.
 - c. **Facoltativo**: Inserisci un gateway.

3. Fare clic su **Crea VLAN**.

Trova maggiori informazioni

[Aggiungi una rete virtuale](#)

Modifica una rete virtuale

È possibile modificare gli attributi VLAN, come il nome VLAN, la netmask e la dimensione dei blocchi di indirizzi IP. Il tag VLAN e SVIP non possono essere modificati per una VLAN. L'attributo gateway non è un parametro valido per le VLAN non VRF.

Se sono presenti sessioni iSCSI, di replica remota o di altra rete, la modifica potrebbe non riuscire.

Quando si gestisce la dimensione degli intervalli di indirizzi IP VLAN, è necessario tenere presenti le seguenti limitazioni:

- È possibile rimuovere gli indirizzi IP solo dall'intervallo di indirizzi IP iniziale assegnato al momento della creazione della VLAN.
- È possibile rimuovere un blocco di indirizzi IP aggiunto dopo l'intervallo di indirizzi IP iniziale, ma non è possibile ridimensionare un blocco IP rimuovendo gli indirizzi IP.
- Quando si tenta di rimuovere indirizzi IP, dall'intervallo di indirizzi IP iniziale o da un blocco IP, utilizzati dai nodi del cluster, l'operazione potrebbe non riuscire.
- Non è possibile riassegnare specifici indirizzi IP in uso ad altri nodi del cluster.

È possibile aggiungere un blocco di indirizzi IP utilizzando la seguente procedura:

1. Selezionare **Cluster > Rete**.
2. Selezionare l'icona Azioni per la VLAN che si desidera modificare.
3. Selezionare **Modifica**.
4. Nella finestra di dialogo **Modifica VLAN**, immettere i nuovi attributi per la VLAN.
5. Selezionare **Aggiungi un blocco** per aggiungere un blocco non continuo di indirizzi IP per la rete virtuale.
6. Selezionare **Salva modifiche**.

Collegamento agli articoli della Knowledge Base sulla risoluzione dei problemi

Collegamento agli articoli della Knowledge Base per assistenza nella risoluzione dei problemi relativi alla gestione degli intervalli di indirizzi IP della VLAN.

- ["Avviso di IP duplicato dopo l'aggiunta di un nodo di archiviazione nella VLAN sul cluster Element"](#)
- ["Come determinare quali IP VLAN sono in uso e a quali nodi sono assegnati tali IP in Element"](#)

Modifica VLAN VRF

È possibile modificare gli attributi VLAN VRF, come il nome VLAN, la netmask, il gateway e i blocchi di indirizzi IP.

1. Fare clic su **Cluster > Rete**.
2. Fare clic sull'icona Azioni per la VLAN che si desidera modificare.

3. Fare clic su **Modifica**.
4. Immettere i nuovi attributi per la VLAN VRF nella finestra di dialogo **Modifica VLAN**.
5. Fare clic su **Salva modifiche**.

Elimina una rete virtuale

È possibile rimuovere un oggetto di rete virtuale. Prima di rimuovere una rete virtuale, è necessario aggiungere i blocchi di indirizzi a un'altra rete virtuale.

1. Fare clic su **Cluster > Rete**.
2. Fare clic sull'icona Azioni relativa alla VLAN che si desidera eliminare.
3. Fare clic su **Elimina**.
4. Conferma il messaggio.

Trova maggiori informazioni

[Modifica una rete virtuale](#)

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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