Gestire il sistema

Element Software

NetApp
October 01, 2024

Sommario

Gestire il sistema

È possibile gestire il sistema nell'interfaccia utente di Element. Ciò include l'abilitazione dell'autenticazione a più fattori, la gestione delle impostazioni del cluster, il supporto degli standard FIPS (Federal Information Processing Standards) e l'utilizzo della gestione esterna delle chiavi.

- "Abilitare l'autenticazione a più fattori"
- "Configurare le impostazioni del cluster"
- "Creare un cluster che supporti i dischi FIPS"
- "Inizia a utilizzare la gestione esterna delle chiavi"

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Abilitare l'autenticazione a più fattori

L'autenticazione a più fattori (MFA) utilizza un provider di identità (IdP) di terze parti tramite il linguaggio SAML (Security Assertion Markup Language) per gestire le sessioni utente. MFA consente agli amministratori di configurare ulteriori fattori di autenticazione, come password e SMS, password e messaggi di posta elettronica.

Impostare l'autenticazione a più fattori

È possibile utilizzare questi passaggi di base tramite l'API Element per configurare il cluster in modo che utilizzi l'autenticazione a più fattori.

I dettagli di ciascun metodo API sono disponibili nella "Riferimento API dell'elemento".

1. Creare una nuova configurazione IdP (Identity Provider) di terze parti per il cluster chiamando il seguente metodo API e passando i metadati IdP in formato JSON: `CreateIdpConfiguration`

   I metadati IDP, in formato testo normale, vengono recuperati da IdP di terze parti. Questi metadati devono essere validati per garantire che siano formattati correttamente in JSON. Sono disponibili numerose applicazioni per formatter JSON, ad esempio:https://freeformatter.com/json-escape.html.

2. Recuperare i metadati del cluster, tramite spMetadataUrl, per copiare nell'IdP di terze parti chiamando il seguente metodo API: `ListIdpConfigurations`

   SpMetadataUrl è un URL utilizzato per recuperare i metadati del provider di servizi dal cluster per IdP al fine di stabilire una relazione di trust.

3. Configurare le asserzioni SAML sull'IdP di terze parti in modo che includa l'attributo "NameID" per identificare in modo univoco un utente per la registrazione dell'audit e per il corretto funzionamento della disconnessione singola.

4. Creare uno o più account utente amministratore cluster autenticati da un IdP di terze parti per l'autorizzazione chiamando il seguente metodo API:`AddIdpClusterAdmin`

   > Il nome utente per l'amministratore del cluster IdP deve corrispondere alla mappatura nome/valore attributo SAML per l'effetto desiderato, come mostrato negli esempi seguenti:

   - Email=bob@company.com — dove IdP è configurato per rilasciare un indirizzo email negli attributi SAML.
   - Group=cluster-Administrator - dove IdP è configurato per rilasciare una proprietà di gruppo in cui tutti gli utenti devono avere accesso. Tenere presente che l'associazione nome attributo/valore SAML è sensibile alla distinzione tra maiuscole e minuscole per motivi di sicurezza.

5. Abilitare MFA per il cluster chiamando il seguente metodo API: `EnableIdpAuthentication`

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Ulteriori informazioni per l'autenticazione a più fattori

È necessario conoscere le seguenti avvertenze relative all'autenticazione a più fattori.

- Per aggiornare i certificati IdP che non sono più validi, è necessario utilizzare un utente amministratore non IdP per chiamare il seguente metodo API: `UpdateIdpConfiguration`
- MFA non è compatibile con i certificati di lunghezza inferiore a 2048 bit. Per impostazione predefinita, nel cluster viene creato un certificato SSL a 2048 bit. Si consiglia di evitare di impostare un certificato di dimensioni inferiori quando si chiama il metodo API: `SetSSLCertificate`

  > Se il cluster utilizza un certificato precedente all'aggiornamento a meno di 2048 bit, il certificato del cluster deve essere aggiornato con un certificato a 2048 bit o superiore dopo l'aggiornamento all'elemento 12.0 o successivo.

- Gli utenti amministratori IDP non possono essere utilizzati per effettuare chiamate API direttamente (ad esempio, tramite SDK o Postman) o per altre integrazioni (ad esempio, OpenStack Cinder o vCenter Plug-in). Aggiungere utenti amministratori cluster LDAP o utenti amministratori cluster locali se si desidera creare utenti con queste funzionalità.

Trova ulteriori informazioni

- "Gestione dello storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Configurare le impostazioni del cluster

È possibile visualizzare e modificare le impostazioni a livello di cluster ed eseguire attività specifiche del cluster dalla scheda Cluster dell'interfaccia utente di Element.

È possibile configurare impostazioni come la soglia di fullness del cluster, l'accesso al supporto, la crittografia

a riposo, i volumi virtuali, SnapMirror, E NTP broadcast client.

Opzioni

- Lavorare con volumi virtuali
- Utilizzare la replica SnapMirror tra cluster Element e ONTAP
- Impostare la soglia completa del cluster
- Abilitare e disabilitare l'accesso al supporto
- "Come vengono calcolate le soglie blockSpace per l'elemento"
- Attivare e disattivare la crittografia per un cluster
- Gestire il banner Termini di utilizzo
- Configurare i server Network Time Protocol per il cluster da interrogare
- Manage SNMP (Gestisci SNMP)
- Gestire i dischi
- Gestire i nodi
- Gestire le reti virtuali
- Visualizza i dettagli delle porte Fibre Channel

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Attivare e disattivare la crittografia a riposo per un cluster

Con i cluster SolidFire, è possibile crittografare tutti i dati inattivi memorizzati sui dischi del cluster. Puoi abilitare una protezione a livello di cluster dei dischi con crittografia automatica (SED) utilizzando una "crittografia basata su hardware o software a riposo"delle due .

È possibile attivare la crittografia hardware a riposo utilizzando l'interfaccia utente o l'API Element. L'attivazione della funzione di crittografia hardware a riposo non influisce sulle prestazioni o sull'efficienza del cluster. È possibile attivare la crittografia software a riposo utilizzando solo l'API Element.

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

> Per i cluster di storage all-flash SolidFire, la crittografia software a riposo deve essere attivata durante la creazione del cluster e non può essere disattivata dopo la creazione del cluster.

Di cosa hai bisogno

- Si dispone dei privilegi di amministratore del cluster per attivare o modificare le impostazioni di crittografia.
- Per la crittografia basata su hardware a riposo, è stato garantito che il cluster sia in buono stato prima di modificare le impostazioni di crittografia.
- Se si disattiva la crittografia, due nodi devono partecipare a un cluster per accedere alla chiave e disattivare la crittografia su un disco.

Controllare la crittografia nello stato di riposo

Per visualizzare lo stato attuale della crittografia a riposo e/o della crittografia software a riposo nel cluster, utilizza il "GetClusterInfo" metodo. Questo metodo consente "GetSoftwareEncryptionAtRestInfo"di ottenere le informazioni utilizzate dal cluster per crittografare i dati inutilizzati.

> Al momento, la dashboard dell'interfaccia utente del software Element `https://<MVIP>/` mostra solo lo stato della crittografia a riposo per la crittografia basata su hardware.

Opzioni

- Abilitare la crittografia basata su hardware a riposo
- Abilitare la crittografia basata su software a riposo
- Disattiva la crittografia basata su hardware a riposo

Abilitare la crittografia basata su hardware a riposo

> Per abilitare la crittografia a riposo utilizzando una configurazione di gestione della chiave esterna, è necessario abilitare la crittografia a riposo tramite "API". L'abilitazione mediante il pulsante Element UI esistente tornerà a utilizzare chiavi generate internamente.

1. Dall'interfaccia utente di Element, selezionare **Cluster** > **Settings**.
2. Selezionare **Enable Encryption at REST (attiva crittografia a riposo)**.

Abilitare la crittografia basata su software a riposo

> La crittografia software a riposo non può essere disattivata dopo che è stata attivata sul cluster.

1. Durante la creazione del cluster, eseguire "creare il metodo del cluster"con `enableSoftwareEncryptionAtRest` impostato su `true`.

Disattiva la crittografia basata su hardware a riposo

1. Dall'interfaccia utente di Element, selezionare **Cluster** > **Settings**.
2. Selezionare **Disattiva crittografia a riposo**.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Impostare la soglia completa del cluster

È possibile modificare il livello con cui il sistema genera un avviso di riempimento del cluster a blocchi seguendo la procedura riportata di seguito. Inoltre, è possibile utilizzare il metodo dell'API ModifyClusterFullThreshold per modificare il livello con cui il sistema genera un avviso di blocco o metadati.

Di cosa hai bisogno

È necessario disporre dei privilegi di amministratore del cluster.

Fasi

1. Fare clic su **Cluster** > **Settings**.
2. Nella sezione Cluster Full Settings (Impostazioni cluster complete), inserire una percentuale in **Raise a warning alert when _% Capacity remains before Helix not recovery from a node failure** (Invia un avviso quando la capacità del _% rimane prima che Helix non possa
3. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

"Come vengono calcolate le soglie blockSpace per l'elemento"

Abilitare e disabilitare 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** > **Settings**.
2. Nella sezione Enable / Disable Support Access (attiva/Disattiva accesso al supporto), immettere la durata (in ore) per la quale si desidera consentire l'accesso al supporto.
3. Fare clic su **Enable Support Access** (attiva accesso supporto).
4. **Opzionale:** per disattivare l'accesso al supporto, fare clic su **Disattiva accesso al supporto**.

Gestire il banner Termini di utilizzo

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

Opzioni

Attivare il banner Termini di utilizzo Modificare il banner Termini di utilizzo Disattiva il banner Termini di utilizzo

Attivare il banner Termini di utilizzo

È possibile attivare un banner Termini di utilizzo che viene visualizzato quando un utente accede all'interfaccia utente di Element. Quando l'utente fa clic sul banner, viene visualizzata una finestra di dialogo contenente il messaggio configurato per il cluster. Il banner può essere ignorato in qualsiasi momento.

Per attivare 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**, inserire il testo da visualizzare nella finestra di dialogo Termini di utilizzo.

   Non superare i 4096 caratteri.

3. Fare clic su **Enable** (attiva).

Modificare il banner Termini di utilizzo

Puoi modificare il testo visualizzato dall'utente quando seleziona il banner di accesso Termini di utilizzo.

Di cosa hai bisogno

- Per configurare le Condizioni d'uso, è necessario disporre dei privilegi di amministratore del cluster.
- Assicurarsi che la funzione Termini di utilizzo sia attivata.

Fasi

1. Fare clic su **utenti** > **Termini di utilizzo**.
2. Nella finestra di dialogo **Termini di utilizzo**, modificare il testo che si desidera visualizzare.

   Non superare i 4096 caratteri.

3. Fare clic su **Save Changes** (Salva modifiche).

Disattiva il banner Termini di utilizzo

È possibile disattivare il banner Termini di utilizzo. Con il banner disattivato, non viene più richiesto all'utente di accettare i termini di utilizzo quando si utilizza l'interfaccia utente di Element.

Di cosa hai bisogno

- Per configurare le Condizioni d'uso, è necessario disporre dei privilegi di amministratore del cluster.
- Assicurarsi che le condizioni d'uso siano attivate.

Fasi

1. Fare clic su **utenti** > **Termini di utilizzo**.
2. Fare clic su **Disable** (Disattiva).

Impostare Network Time Protocol

L'impostazione del protocollo NTP (Network Time Protocol) può essere eseguita in due modi: Istruire ciascun nodo di un cluster a rimanere in attesa delle trasmissioni o richiedere a ciascun nodo di eseguire una query su un server NTP per gli aggiornamenti.

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

Configurare i server Network Time Protocol per il cluster da interrogare

È possibile richiedere a ciascun nodo di un cluster di eseguire query su un server NTP (Network Time Protocol) per gli aggiornamenti. Il cluster contatta solo i server configurati e richiede informazioni NTP.

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, non è sempre possibile stabilire una connessione a questo sito a seconda della posizione fisica del cluster SolidFire.

L'utilizzo dell'FQDN dipende dal fatto che le impostazioni DNS del singolo nodo di storage siano state

configurate e operative. A tale scopo, configurare i server DNS su ogni nodo di storage e assicurarsi che le porte siano aperte consultando la pagina requisiti della porta di rete.

È possibile inserire fino a cinque server NTP diversi.

È possibile utilizzare indirizzi IPv4 e IPv6.

Di cosa hai bisogno

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

Fasi

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** > **Settings**.
4. In Network Time Protocol Settings (Impostazioni protocollo ora di rete), selezionare **No**, che utilizza la configurazione NTP standard.
5. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Configurare il cluster in modo che sia in attesa di trasmissioni NTP

Utilizzando la modalità di trasmissione, è possibile impostare ciascun nodo di un cluster in modo che ascolti sulla rete i messaggi di trasmissione NTP (Network Time Protocol) provenienti da un determinato server.

Di cosa hai bisogno

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

Fasi

1. Fare clic su **Cluster** > **Settings**.
2. Inserire il server NTP o i server che utilizzano la modalità di trasmissione nell'elenco dei server.
3. In Network Time Protocol Settings (Impostazioni protocollo ora di rete), selezionare **Yes** (Sì) per utilizzare un client di trasmissione.
4. Per impostare il client di trasmissione, nel campo **Server**, immettere il server NTP configurato in modalità broadcast.
5. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Manage SNMP (Gestisci 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 del modello di protezione basato sull'utente SNMP e configurare i trap per monitorare il cluster SolidFire. È inoltre possibile visualizzare e accedere ai file della base di informazioni di gestione.

È possibile utilizzare indirizzi IPv4 e 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 attivare o disattivare SNMP. Dopo aver attivato SNMP, è possibile scegliere la versione da utilizzare. Se si utilizza la versione 2, è possibile aggiungere i requestori e, se si utilizza la versione 3, è possibile configurare gli utenti USM.

- **SNMP Trap Settings** (Impostazioni trap SNMP)

  È possibile identificare le trap che si desidera acquisire. È possibile impostare l'host, la porta e la stringa di comunità per ciascun destinatario del trap.

Configurare un richiedente SNMP

Quando SNMP versione 2 è attivato, è possibile attivare o disattivare un richiedente e configurare i requestori per ricevere richieste SNMP autorizzate.

1. Fare clic su **Cluster › SNMP**.
2. In **General SNMP Settings** (Impostazioni SNMP generali), fare clic su **Yes** (Sì) per attivare SNMP.
3. Dall'elenco **Version** (versione), selezionare **Version 2** (versione 2).
4. Nella sezione **Requestori**, inserire le informazioni **stringa di comunità** e **rete**.

   Per impostazione predefinita, la stringa di comunità è pubblica e la rete è localhost. È possibile modificare queste impostazioni predefinite.

5. **Opzionale:** per aggiungere un altro richiedente, fare clic su **Aggiungi richiedente** e immettere le informazioni **stringa di comunità** e **rete**.
6. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

- Configurare i trap SNMP
- Visualizzare i dati degli oggetti gestiti utilizzando i file della base di informazioni di gestione

Configurare un utente SNMP USM

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

1. Fare clic su **Cluster** > **SNMP**.
2. In **General SNMP Settings** (Impostazioni SNMP generali), fare clic su **Yes** (Sì) per attivare SNMP.
3. Dall'elenco **Version** (versione), selezionare **Version 3** (versione 2).
4. Nella sezione **utenti USM**, immettere il nome, la password e la passphrase.
5. **Opzionale:** per aggiungere un altro utente USM, fare clic su **Aggiungi utente USM** e inserire il nome, la password e la passphrase.
6. Fare clic su **Save Changes** (Salva modifiche).

Configurare i trap SNMP

Gli amministratori di sistema possono utilizzare i trap SNMP, definiti anche notifiche, per monitorare lo stato del cluster SolidFire.

Quando i trap SNMP sono attivati, il cluster SolidFire genera trap associati alle voci del registro eventi e agli avvisi di sistema. Per ricevere notifiche SNMP, è necessario scegliere i trap da generare e identificare i destinatari delle informazioni trap. Per impostazione predefinita, non viene generato alcun trap.

1. Fare clic su **Cluster** > **SNMP**.
2. Selezionare uno o più tipi di trap nella sezione **Impostazioni trap SNMP** che il sistema deve generare:
   - Trap di guasti del cluster
   - Trap di guasti risolti nel cluster
   - Trap di eventi del cluster
3. Nella sezione **destinatari trap**, immettere le informazioni relative a host, porta e community string per un destinatario.
4. **Opzionale**: Per aggiungere un altro destinatario trap, fare clic su **Aggiungi destinatario trap** e immettere le informazioni relative a host, porta e stringa di comunità.
5. Fare clic su **Save Changes** (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 dei volumi
- Volumi per statistiche account
- Statistiche dei nodi
- Altri dati, ad esempio report, errori ed eventi di sistema

Il sistema supporta anche l'accesso al file MIB contenente gli access point di livello superiore (OID) per i prodotti SF-Series.

Fasi

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

Gestire i dischi

Ogni nodo contiene uno o più dischi fisici utilizzati per memorizzare una parte dei dati per il cluster. Il cluster utilizza la capacità e le prestazioni del disco dopo che il disco è stato aggiunto correttamente a un cluster. È possibile utilizzare l'interfaccia utente Element per gestire i dischi.

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Dettagli sui dischi

La pagina Drives (unità) della scheda Cluster (cluster) fornisce un elenco dei dischi attivi nel cluster. È possibile filtrare la pagina selezionando dalle 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 dischi non assegnati a un cluster ed elencati nella scheda Available (disponibili) dopo la creazione di un nuovo cluster SolidFire.

I seguenti elementi vengono visualizzati nell'elenco dei dischi attivi.

- **ID unità**

  Il numero sequenziale assegnato al disco.

- **ID nodo**

  Il numero di nodo assegnato quando il nodo viene aggiunto al cluster.

- **Nome nodo**

  Il nome del nodo che ospita l'unità.

- **Slot**

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

- **Capacità**

  Le dimensioni del disco, in GB.

- **Seriale**

  Il numero di serie del disco.

- **Usura residua**

  L'indicatore del livello di usura.

  Il sistema storage indica la quantità approssimativa di usura disponibile su ogni disco a stato solido (SSD) per la scrittura e la cancellazione dei dati. Un disco che ha consumato il 5% dei cicli di scrittura e cancellazione progettati riporta il 95% di usura rimanente. Il sistema non aggiorna automaticamente le informazioni sull'usura del disco; è possibile aggiornare o chiudere e ricaricare la pagina per aggiornare le informazioni.

- **Tipo**

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

Gestire i nodi

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

Se un nodo aggiunto di recente rappresenta oltre il 50% della capacità totale del cluster, una parte della capacità di questo nodo viene resa inutilizzabile ("bloccato"), in modo che sia conforme alla regola di capacità. Questo rimane il caso fino a quando non viene aggiunto ulteriore storage. Se viene aggiunto un nodo molto grande che disobbedisce anche alla regola di capacità, il nodo precedentemente bloccato non verrà più bloccato, mentre il nodo appena aggiunto viene bloccato. La capacità deve essere sempre aggiunta in coppie per evitare che ciò accada. Quando un nodo viene bloccato, viene generato un guasto appropriato del cluster.

Trova ulteriori informazioni

Aggiungere un nodo a un cluster

Aggiungere un nodo a un cluster

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

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

È possibile aggiungere nodi di capacità inferiore o superiore 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 spostare i dati in

modo da lasciare spazio sufficiente in caso di guasto di uno dei nodi più grandi. È possibile aggiungere capacità di nodo inferiori a un cluster di nodi più grande per migliorare le performance.

> Se un nodo aggiunto di recente rappresenta oltre il 50% della capacità totale del cluster, una parte della capacità di questo nodo viene resa inutilizzabile ("bloccato"), in modo che sia conforme alla regola di capacità. Questo rimane il caso fino a quando non viene aggiunto ulteriore storage. Se viene aggiunto un nodo molto grande che disobbedisce anche alla regola di capacità, il nodo precedentemente bloccato non verrà più bloccato, mentre il nodo appena aggiunto viene bloccato. La capacità deve essere sempre aggiunta in coppie per evitare che ciò accada. Quando un nodo viene bloccato, viene generato l'errore del cluster strandedCapacity.

"Video di NetApp: Scalabilità in base ai termini: Espansione di un cluster SolidFire"

È possibile aggiungere nodi alle appliance NetApp HCI.

Fasi

1. Selezionare **Cluster** > **Nodes**.
2. Fare clic su **Pending** (in sospeso) per visualizzare l'elenco dei nodi in sospeso.

   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 Pending Active (attivo in sospeso).

   SolidFire installa la versione software Element del cluster sui nodi in sospeso quando vengono aggiunti a un cluster. L'operazione potrebbe richiedere alcuni minuti.

3. Effettuare una delle seguenti operazioni:
   - Per aggiungere singoli nodi, fare clic sull'icona **azioni** del nodo che si desidera aggiungere.
   - Per aggiungere più nodi, selezionare la casella di controllo dei nodi da aggiungere, quindi **azioni in blocco**. **Nota:** se il nodo che si sta 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. Una volta aggiornato, il nodo si aggiunge automaticamente al cluster. Durante questo processo asincrono, il nodo si trova in uno stato Active pendingActive.
4. Fare clic su **Aggiungi**.

   Il nodo viene visualizzato nell'elenco dei nodi attivi.

Trova ulteriori informazioni

Versione e compatibilità dei nodi

Versione e compatibilità dei nodi

La compatibilità dei nodi si basa sulla versione software di Element installata su un nodo. I cluster di storage basati su software Element imbasano automaticamente un'immagine di un nodo alla versione software Element sul cluster se il nodo e il cluster non sono compatibili.

Il seguente elenco descrive i livelli di importanza delle release software che compongono il numero di versione del software Element:

- **Maggiore**

  Il primo numero indica una versione 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 può essere creato un cluster con nodi con versioni principali miste.

- **Minore**

  Il secondo numero indica funzionalità software più piccole o miglioramenti alle funzionalità software esistenti che sono state aggiunte a una release principale. Questo componente viene incrementato all'interno di un componente di versione principale per indicare che questa release incrementale non è compatibile con altre release incrementali di software elemento con un componente minore 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 software dell'elemento rappresentata dai componenti major.minor. Ad esempio, 11.0.1 è compatibile con 11.0 e 11.0.2 con 11.0.3.

I numeri di versione principali e secondari devono corrispondere per la compatibilità. I micro numeri non devono corrispondere per la compatibilità.

Capacità del cluster in un ambiente a nodi misti

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

La serie H è composta da nodi H610S-1, H610S-2, H610S-4 e H410S. Questi nodi sono entrambi compatibili con 10 GbE e 25 GbE.

Si consiglia di non mischiare nodi non crittografati e crittografati. In un cluster a nodi misti, nessun nodo può superare il 33% 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 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 storage SF-Series non sono supportati:

A partire da…	Nodo storage non supportato…
Elemento 12,7	• SF2405 • SF9608
Elemento 12,0	• SF3010 • SF6010 • SF9010

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

Visualizza i dettagli del nodo

È possibile visualizzare i dettagli dei singoli nodi, ad esempio i tag di servizio, i dettagli dei dischi e la grafica per l'utilizzo e le statistiche dei dischi. La pagina nodi della scheda Cluster fornisce la colonna Version (versione) in cui è possibile visualizzare la versione software di ciascun nodo.

Fasi

1. Fare clic su **Cluster** > **Nodes**.
2. Per visualizzare i dettagli di un nodo specifico, fare clic sull'icona **azioni** di un nodo.
3. Fare clic su **View Details** (Visualizza dettagli).
4. Esaminare i dettagli del nodo:
   - **Node ID**: L'ID generato dal sistema per il nodo.
   - **Node Name** (Nome nodo): Il nome host del nodo.
   - **IOPS 4k disponibili**: Gli IOPS configurati per il nodo.
   - **Node role**: Ruolo del nodo nel cluster. Valori possibili:
     - Cluster Master: Nodo che esegue attività amministrative a livello di cluster e contiene MVIP e SVIP.
     - Ensemble Node: Nodo che partecipa al cluster. Esistono 3 o 5 nodi di ensemble a seconda delle dimensioni del cluster.
     - Fibre Channel: Un nodo nel cluster.
   - **Node Type**: Il tipo di modello del nodo.
   - **Active Drives**: Il numero di dischi attivi nel nodo.
   - **IP di gestione**: L'indirizzo IP di gestione (MIP) assegnato al nodo per le attività di amministrazione della rete da 1 GbE o 10 GbE.
   - **Cluster IP**: L'indirizzo IP del cluster (CIP) assegnato al nodo utilizzato per la comunicazione tra i nodi dello stesso cluster.
   - **Storage IP**: L'indirizzo IP (SIP) dello storage assegnato al nodo utilizzato per il rilevamento della rete iSCSI e per tutto il traffico della rete dati.
   - **Management VLAN ID** (ID VLAN di gestione): L'ID virtuale per la rete locale di gestione.
   - **Storage VLAN ID**: L'ID virtuale per la rete locale di storage.
   - **Version**: La versione del software in esecuzione su ciascun nodo.
   - **Replication Port** (porta di replica): La porta utilizzata sui nodi per la replica remota.
   - **Service Tag**: Numero di service tag univoco assegnato al nodo.

Visualizza i dettagli delle porte Fibre Channel

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

Consente di visualizzare informazioni sulle porte Fibre Channel collegate al cluster.

Fasi

1. Fare clic su **Cluster** > **FC Ports**.

2. Per filtrare le informazioni in questa pagina, fare clic su **Filter** (filtro).
3. Leggi i dettagli:
    - **Node ID**: Il nodo che ospita la sessione per la connessione.
    - **Node Name**: Nome del nodo generato dal sistema.
    - **Slot**: Numero dello slot in cui si trova la porta Fibre Channel.
    - **HBA Port**: Porta fisica sull'HBA (host bus adapter) Fibre Channel.
    - **WWNN**: Il nome del nodo mondiale.
    - **WWPN**: Il nome della porta universale di destinazione.
    - **Switch WWN**: Nome mondiale dello switch Fibre Channel.
    - **Port state** (Stato porta): Stato corrente della porta.
    - **NID porta**: L'ID della porta del nodo sul fabric Fibre Channel.
    - **Speed**: La velocità negoziata di Fibre Channel. I valori possibili sono i seguenti:
        - 4Gbps
        - 8Gbps
        - 16Gbps

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Gestire le reti virtuali

Il networking virtuale nello storage SolidFire consente di connettere il traffico tra più client su reti logiche separate a un cluster. Le connessioni al cluster vengono separate nello stack di rete attraverso l'utilizzo del tagging VLAN.

Trova ulteriori informazioni

- Aggiungere una rete virtuale
- Abilitare il routing e l'inoltro virtuale
- Modificare una rete virtuale
- Modificare le VLAN VRF
- Eliminare una rete virtuale

Aggiungere una rete virtuale

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

Di cosa hai bisogno

- Identificare il blocco di indirizzi IP che verranno assegnati alle reti virtuali sui nodi del cluster.

- Identificare un indirizzo IP della rete di storage (SVIP) che verrà utilizzato come endpoint per tutto il traffico dello storage NetApp Element.

Per questa configurazione, è necessario prendere in considerazione i seguenti criteri:

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

Quando viene aggiunta una rete virtuale, viene creata un'interfaccia per ciascun nodo e ciascun nodo richiede un indirizzo IP della rete virtuale. Il numero di indirizzi IP specificati durante la creazione di una nuova rete virtuale deve essere uguale o superiore al numero di nodi nel cluster. Gli indirizzi delle reti virtuali vengono forniti in blocco e assegnati automaticamente ai singoli nodi. Non è necessario assegnare manualmente gli indirizzi di rete virtuale ai nodi nel cluster.

Fasi

1. Fare clic su **Cluster** > **Network**.
2. Fare clic su **Create VLAN** (Crea VLAN).
3. Nella finestra di dialogo **Crea una nuova VLAN**, immettere i valori nei seguenti campi:
   - **Nome VLAN**
   - **Tag VLAN**
   - **SVIP**
   - **Netmask**
   - (Facoltativo) **Descrizione**
4. Inserire l'indirizzo **IP iniziale** per l'intervallo di indirizzi IP in **blocchi di indirizzi IP**.
5. Inserire **Size** dell'intervallo IP come numero di indirizzi IP da includere nel blocco.
6. Fare clic su **Add a block** (Aggiungi un blocco) per aggiungere un blocco non continuo di indirizzi IP per questa VLAN.
7. Fare clic su **Create VLAN** (Crea VLAN).

Visualizza i dettagli della rete virtuale

Fasi

1. Fare clic su **Cluster** > **Network**.
2. Esaminare i dettagli.
   - **ID**: ID univoco della rete VLAN, assegnato dal sistema.
   - **Name**: Nome univoco assegnato dall'utente per la rete VLAN.
   - **VLAN Tag**: Tag VLAN assegnato al momento della creazione della rete virtuale.
   - **SVIP**: Indirizzo IP virtuale dello storage assegnato alla rete virtuale.
   - **Netmask**: Netmask per questa rete virtuale.
   - **Gateway**: Indirizzo IP univoco di un gateway di rete virtuale. VRF deve essere attivato.
   - **VRF Enabled**: Indicazione dell'attivazione o meno del routing e dell'inoltro virtuale.

- **IP utilizzati**: Intervallo di indirizzi IP della rete virtuale utilizzati per la rete virtuale.

Abilitare il routing e l'inoltro virtuale

È possibile attivare il routing e l'inoltro virtuale (VRF), che consente a più istanze di una tabella di routing di esistere in un router e di lavorare contemporaneamente. Questa funzionalità è disponibile solo per le reti di storage.

È possibile attivare 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** > **Network**.
2. Per attivare VRF su una nuova VLAN, selezionare **Create VLAN** (Crea VLAN).
   a. Inserire le informazioni pertinenti per la nuova VRF/VLAN. Vedere aggiunta di una rete virtuale.
   b. Selezionare la casella di controllo **Enable VRF** (attiva SNMP).
   c. **Opzionale**: Inserire un gateway.
3. Fare clic su **Create VLAN** (Crea VLAN).

Trova ulteriori informazioni

Aggiungere una rete virtuale

Modificare una rete virtuale

È possibile modificare gli attributi della VLAN, ad esempio il nome della 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 iSCSI, replica remota o altre sessioni di rete, la modifica potrebbe non riuscire.

Quando si gestiscono le dimensioni degli intervalli di indirizzi IP della VLAN, 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 gli indirizzi IP, dall'intervallo di indirizzi IP iniziale o in un blocco IP, utilizzati dai nodi nel cluster, l'operazione potrebbe non riuscire.
- Non è possibile riassegnare indirizzi IP in uso specifici ad altri nodi nel cluster.

È possibile aggiungere un blocco di indirizzi IP seguendo la procedura riportata di seguito:

1. Selezionare **Cluster** > **Network**.
2. Selezionare l'icona Actions (azioni) per la VLAN che si desidera modificare.
3. Selezionare **Modifica**.
4. Nella finestra di dialogo **Edit VLAN** (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 **Save Changes** (Salva modifiche).

Collegamento agli articoli della Knowledge base per la 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 IP duplicato dopo l'aggiunta di un nodo di storage nella VLAN sul cluster di elementi"
- "Come determinare quali IP VLAN sono in uso e a quali nodi sono assegnati in Element"

Modificare le VLAN VRF

È possibile modificare gli attributi della VLAN VRF, ad esempio nome VLAN, netmask, gateway e blocchi di indirizzi IP.

1. Fare clic su **Cluster** > **Network**.
2. Fare clic sull'icona Actions (azioni) per la VLAN che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Inserire i nuovi attributi per la VLAN VRF nella finestra di dialogo **Edit VLAN** (Modifica VLAN).
5. Fare clic su **Save Changes** (Salva modifiche).

Eliminare una rete virtuale

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

1. Fare clic su **Cluster** > **Network**.
2. Fare clic sull'icona Actions (azioni) per la VLAN che si desidera eliminare.
3. Fare clic su **Delete** (Elimina).
4. Confermare il messaggio.

Trova ulteriori informazioni

Modificare una rete virtuale

Creare un cluster che supporti i dischi FIPS

La sicurezza sta diventando sempre più critica per l'implementazione di soluzioni in molti ambienti dei clienti. Gli standard FIPS (Federal Information Processing Standards) sono standard per la sicurezza e l'interoperabilità dei computer. La crittografia certificata FIPS 140-2 per i dati inattivi è un componente della soluzione di sicurezza globale.

- "Evitare la combinazione di nodi per i dischi FIPS"
- "Abilitare la crittografia a riposo"
- "Identificare se i nodi sono pronti per la funzionalità dei dischi FIPS"
- "Attivare la funzione dischi FIPS"

- "Controllare lo stato del disco FIPS"
- "Risolvere i problemi relativi alla funzione del disco FIPS"

Evitare la combinazione di nodi per i dischi FIPS

Per prepararsi all'attivazione della funzione dischi FIPS, evitare di combinare nodi in cui alcuni sono in grado di supportare dischi FIPS e altri no.

Un cluster è considerato conforme ai dischi FIPS in base alle seguenti condizioni:

- Tutti i dischi sono certificati come dischi FIPS.
- Tutti i nodi sono nodi di dischi FIPS.
- La crittografia a riposo (EAR) è attivata.
- La funzione dischi FIPS è attivata. Tutti i dischi e i nodi devono essere compatibili con FIPS e la crittografia a riposo deve essere attivata per abilitare la funzione disco FIPS.

Abilitare la crittografia a riposo

È possibile attivare e disattivare la crittografia a livello di cluster a riposo. Questa funzione non è attivata per impostazione predefinita. Per supportare le unità FIPS, è necessario attivare la crittografia a riposo.

1. Nell'interfaccia utente del software NetApp Element, fare clic su **cluster** > **Impostazioni**.
2. Fare clic su *Enable Encryption at REST (attiva crittografia a riposo)

Trova ulteriori informazioni

- Attivare e disattivare la crittografia per un cluster
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Identificare se i nodi sono pronti per la funzionalità dei dischi FIPS

Verificare se tutti i nodi del cluster di storage sono pronti a supportare le unità FIPS utilizzando il metodo API GetFipsReport del software NetApp Element.

Il report risultante mostra uno dei seguenti stati:

- None (Nessuna): Il nodo non è in grado di supportare la funzione dei dischi FIPS.
- Parziale: Il nodo è compatibile con FIPS, ma non tutti i dischi sono dischi FIPS.
- Pronto: Il nodo è compatibile con FIPS e tutti i dischi sono dischi FIPS o non sono presenti dischi.

Fasi

1. Utilizzando l'API Element, verificare se i nodi e i dischi nel cluster di storage sono in grado di utilizzare dischi FIPS immettendo:

   ```
   GetFipsReport
   ```

2. Esaminare i risultati, prendendo nota di eventuali nodi che non hanno visualizzato lo stato Ready (Pronto).
3. Per i nodi che non hanno visualizzato lo stato Ready, verificare se il disco è in grado di supportare la funzione dei dischi FIPS:
   - Utilizzando l'API Element, immettere: `GetHardwareList`
   - Annotare il valore di **DriveEncryptionCapabilityType**. Se si tratta di "fips", l'hardware può supportare la funzione dei dischi FIPS.

     Vedere i dettagli su `GetFipsReport` o `ListDriveHardware` nella "Riferimento API dell'elemento".
4. Se il disco non supporta la funzione dischi FIPS, sostituire l'hardware con hardware FIPS (nodo o dischi).

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Attivare la funzione dischi FIPS

È possibile attivare la funzione unità FIPS utilizzando il metodo API software NetApp Element `EnableFeature`.

La crittografia a riposo deve essere attivata sul cluster e tutti i nodi e le unità devono essere compatibili con FIPS, come indicato quando GetFipsReport visualizza uno stato Ready per tutti i nodi.

Fase

1. Utilizzando l'API Element, abilitare FIPS su tutti i dischi immettendo:

   ```
   EnableFeature params: FipsDrives
   ```

Trova ulteriori informazioni

- "Gestire lo storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Controllare lo stato del disco FIPS

È possibile verificare se la funzionalità dischi FIPS è abilitata sul cluster utilizzando il metodo API software NetApp Element `GetFeatureStatus`, che indica se lo stato dischi FIPS abilitati è vero o falso.

1. Utilizzando l'API Element, verificare la funzione dei dischi FIPS nel cluster immettendo:

   ```
   GetFeatureStatus
   ```

2. Esaminare i risultati della `GetFeatureStatus` chiamata API. Se il valore FIPS Drives Enabled (dischi FIPS attivati) è True (vero), la funzione FIPS Drives (dischi FIPS) è attivata.

```
{"enabled": true,
"feature": "FipsDrives"
}
```

Trova ulteriori informazioni

- "Gestire lo storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Risolvere i problemi relativi alla funzione del disco FIPS

Utilizzando l'interfaccia utente del software NetApp Element, è possibile visualizzare avvisi per informazioni su errori o guasti del cluster nel sistema correlati alla funzione dischi FIPS.

1. Utilizzando l'interfaccia utente di Element, selezionare **Reporting** > **Alerts**.
2. Individuare eventuali guasti del cluster, tra cui:
   - Dischi FIPS non corrispondenti
   - FIPS non rispetta la conformità
3. Per suggerimenti sulla risoluzione, vedere informazioni sul codice di errore del cluster.

Trova ulteriori informazioni

- Codici di guasto del cluster
- "Gestire lo storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Abilitare FIPS 140-2 per HTTPS sul cluster

È possibile utilizzare il metodo API EnableFeature per attivare la modalità operativa FIPS 140-2 per le comunicazioni HTTPS.

Con il software NetApp Element, è possibile attivare la modalità operativa FIPS (Federal Information Processing Standards) 140-2 sul cluster. L'attivazione di questa modalità attiva il modulo di protezione crittografica NetApp (NCSM) e sfrutta la crittografia certificata FIPS 140-2 livello 1 per tutte le comunicazioni tramite HTTPS verso l'interfaccia utente e l'API NetApp Element.

Una volta attivata la modalità FIPS 140-2, non è possibile disattivarla. Quando la modalità FIPS 140-2 è attivata, ciascun nodo del cluster si riavvia ed esegue un autotest che garantisce che NCSM sia abilitato e funzioni correttamente nella modalità certificata FIPS 140-2. Ciò causa un'interruzione delle connessioni di gestione e di storage sul cluster. È necessario pianificare attentamente e attivare questa modalità solo se l'ambiente richiede il meccanismo di crittografia che offre.

Per ulteriori informazioni, vedere le informazioni sull'API Element.

Di seguito viene riportato un esempio della richiesta API per attivare FIPS:

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "fips"
    },
    "id": 1
}
```

Una volta attivata questa modalità operativa, tutte le comunicazioni HTTPS utilizzano le crittografia approvate da FIPS 140-2.

Trova ulteriori informazioni

- Crittografie SSL
- "Gestire lo storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Crittografie SSL

Le crittografie SSL sono algoritmi di crittografia utilizzati dagli host per stabilire una comunicazione sicura. Esistono cifrari standard supportati dal software Element e non standard quando è attivata la modalità FIPS 140-2.

I seguenti elenchi forniscono le crittografie standard SSL (Secure Socket Layer) supportate dal software Element e le crittografie SSL supportate quando la modalità FIPS 140-2 è attivata:

- **FIPS 140-2 disattivato**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (DH 2048) - A.

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A.

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) - C.

TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A.

TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A.

TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A.

TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A.

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_IDEA_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_RC4_128_MD5 (RSA 2048) - C.

TLS_RSA_WITH_RC4_128_SHA (RSA 2048) - C.

TLS_RSA_WITH_SEED_CBC_SHA (RSA 2048) - A.

- **FIPS 140-2 abilitato**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (DH 2048) - A.

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECT571R1) - A.

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) - C.

  TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A.

TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A.

TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A.

TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A.

Trova ulteriori informazioni

Abilitare FIPS 140-2 per HTTPS sul cluster

Inizia a utilizzare la gestione esterna delle chiavi

EKM (External Key Management) offre una gestione sicura delle chiavi di autenticazione (AK) insieme a un server esterno delle chiavi (EKS) off-cluster. Gli AKS vengono utilizzati per bloccare e sbloccare i dischi con crittografia automatica (SED) quando "crittografia a riposo" è attivato sul quadro strumenti. EKS fornisce generazione e storage sicuri di AKS. Il cluster utilizza il protocollo KMIP (Key Management Interoperability Protocol), un protocollo standard definito DA OASIS, per comunicare con EKS.

- "Configurare la gestione esterna"
- "Ridigita la chiave master di crittografia software a riposo"
- "Ripristino di chiavi di autenticazione inaccessibili o non valide"
- "Comandi API esterni per la gestione delle chiavi"

Trova ulteriori informazioni

- "API CreateCluster che può essere utilizzata per attivare la crittografia software a riposo"
- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Impostare la gestione esterna delle chiavi

È possibile seguire questi passaggi e utilizzare i metodi API Element elencati per configurare la funzione di gestione delle chiavi esterna.

Di cosa hai bisogno

- Se stai configurando la gestione delle chiavi esterne in combinazione con la crittografia software a riposo, hai abilitato la crittografia software a riposo usando il "CreateCluster"metodo su un nuovo cluster che non contiene volumi.

Fasi

1. Stabilire una relazione di trust con EKS (External Key Server).
   a. Creare una coppia di chiavi pubbliche/private per il cluster di elementi utilizzato per stabilire una relazione di trust con il server delle chiavi chiamando il seguente metodo API: "CreatePublicPrivateKeyPair"

b. Ottenere la richiesta di firma del certificato (CSR) che l'autorità di certificazione deve firmare. La CSR consente al server delle chiavi di verificare che il cluster di elementi che accederà alle chiavi sia autenticato come cluster di elementi. Chiamare il seguente metodo API: "GetClientCertificateSignRequest"

c. Utilizzare EKS/Certificate Authority per firmare la CSR recuperata. Per ulteriori informazioni, consultare la documentazione di terze parti.

2. Creare un server e un provider sul cluster per comunicare con EKS. Un provider di chiavi definisce dove ottenere una chiave e un server definisce gli attributi specifici di EKS con cui verrà comunicata.

a. Creare un provider chiave in cui risiedono i dettagli del server chiave chiamando il seguente metodo API: "CreateKeyProviderKmip"

b. Creare un server delle chiavi che fornisca il certificato firmato e il certificato della chiave pubblica dell'autorità di certificazione chiamando i seguenti metodi API: "CreateKeyServerKmip" "TestKeyServerKmip"

Se il test non riesce, verificare la connettività e la configurazione del server. Quindi ripetere il test.

c. Aggiungere il server delle chiavi nel contenitore del provider di chiavi chiamando i seguenti metodi API: "AddKeyServerToProviderKmip" "TestKeyProviderKmip"

Se il test non riesce, verificare la connettività e la configurazione del server. Quindi ripetere il test.

3. Eseguire una delle seguenti operazioni come fase successiva per la crittografia a riposo:

a. (Per la crittografia hardware a riposo) attivare l'"crittografia hardware a riposo"opzione fornendo l'ID del provider di chiavi che contiene il server di chiavi utilizzato per l'archiviazione delle chiavi chiamando il "EnableEncryptionAtRest"metodo API.

> È necessario abilitare la crittografia a riposo tramite "API". Attivando la crittografia a riposo utilizzando il pulsante dell'interfaccia utente Element esistente, la funzione torna a utilizzare le chiavi generate internamente.

b. (Per la crittografia software a riposo) per poter "crittografia software a riposo"utilizzare il provider di chiavi appena creato, passare l'ID del provider di chiavi al "RekeySoftwareEncryptionAtRestMasterKey"metodo API.

Trova ulteriori informazioni

- "Attivare e disattivare la crittografia per un cluster"
- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Ridigita la chiave master di crittografia software a riposo

È possibile utilizzare l'API Element per reimmettere una chiave esistente. Questo processo crea una nuova chiave master sostitutiva per il server di gestione delle chiavi esterno. Le chiavi master vengono sempre sostituite da nuove chiavi master e non vengono mai duplicate o sovrascritte.

Potrebbe essere necessario eseguire una nuova chiave nell'ambito di una delle seguenti procedure:

- Creare una nuova chiave come parte di un cambiamento dalla gestione interna delle chiavi alla gestione

esterna delle chiavi.

- Creare una nuova chiave come reazione o come protezione contro un evento correlato alla sicurezza.

> Questo processo è asincrono e restituisce una risposta prima del completamento dell'operazione di rekey. È possibile utilizzare il "GetAsyncResult"metodo per eseguire il polling del sistema per verificare il completamento del processo.

Di cosa hai bisogno

- Hai abilitato la crittografia software a riposo usando "CreateCluster"un metodo su un nuovo cluster che non contiene volumi e non dispone di i/O. Utilizzare il collegamento:./api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] per confermare che lo stato è `enabled` prima di procedere.
- Hai scelto "instaurazione di una relazione di fiducia" tra il cluster SolidFire e un server chiavi esterno (EKS). Eseguire il "TestKeyProviderKmip" metodo per verificare che sia stata stabilita una connessione al provider di chiavi.

Fasi

1. Eseguire il "ListKeyProvidersKmip" comando e copiare l'ID del provider di chiavi (`keyProviderID`).
2. Eseguire "RekeySoftwareEncryptionAtRestMasterKey"con il `keyManagementType` parametro AS `external` e `keyProviderID` come numero ID del provider della chiave dal passaggio precedente:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

3. Copiare il `asyncHandle` valore dalla `RekeySoftwareEncryptionAtRestMasterKey` risposta del comando.
4. Eseguire il "GetAsyncResult" comando con il `asyncHandle` valore del passaggio precedente per confermare la modifica della configurazione. Dalla risposta del comando, dovresti vedere che la configurazione della vecchia chiave master è stata aggiornata con le nuove informazioni sulla chiave. Copiare il nuovo ID del provider di chiavi per utilizzarlo in un passaggio successivo.

```
{
   "id": null,
   "result": {
     "createTime": "2021-01-01T22:29:18Z",
     "lastUpdateTime": "2021-01-01T22:45:51Z",
     "result": {
       "keyToDecommission": {
         "keyID": "<value>",
         "keyManagementType": "internal"
     },
     "newKey": {
       "keyID": "<value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "operation": "Rekeying Master Key. Master Key management being
transferred from Internal Key Management to External Key Management with
keyProviderID=<value>",
     "state": "Ready"
   },
   "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
   "status": "complete"
}
```

5. Eseguire `GetSoftwareEncryptionatRestInfo` il comando per confermare che i nuovi dettagli della chiave, compresa la `keyProviderID`, siano stati aggiornati.

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

Trova ulteriori informazioni

- "Gestire lo storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Ripristino di chiavi di autenticazione inaccessibili o non valide

Occasionalmente, può verificarsi un errore che richiede l'intervento dell'utente. In caso di errore, viene generato un guasto del cluster (indicato come codice di guasto del cluster). I due casi più probabili sono descritti qui.

Il cluster non è in grado di sbloccare i dischi a causa di un errore del cluster KmipServerFault.

Questo può verificarsi quando il cluster si avvia per la prima volta e il server delle chiavi non è accessibile o la chiave richiesta non è disponibile.

1. Seguire le fasi di ripristino riportate nei codici di guasto del cluster (se presenti).

Un errore sliceServiceUnhealthy potrebbe essere impostato perché i dischi metadati sono stati contrassegnati come guasti e posizionati nello stato "Available" (disponibile).

Procedura per la cancellazione:

1. Aggiungere di nuovo i dischi.
2. Dopo 3 - 4 minuti, verificare che l' `sliceServiceUnhealthy`anomalia sia stata cancellata.

Per ulteriori informazioni, vedere "codici di guasto del cluster" .

Comandi API esterni per la gestione delle chiavi

Elenco di tutte le API disponibili per la gestione e la configurazione di EKM.

Utilizzato per stabilire una relazione di trust tra il cluster e i server esterni di proprietà del cliente:

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

Utilizzato per definire i dettagli specifici dei server esterni di proprietà del cliente:

- CreateKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServerKmip
- TestKeyServerKmip

Utilizzato per la creazione e la manutenzione di provider di chiavi che gestiscono server di chiavi esterni:

- CreateKeyProviderKmip
- DeleteKeyProviderKmip

- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

Per informazioni sui metodi API, vedere "Informazioni di riferimento API".

Informazioni sul copyright

Informazioni sul marchio commerciale