Utilizzare i comandi "sostituzione controller di sistema" per aggiornare l'hardware del controller introdotto in ONTAP 9.15.1

Upgrade controllers

NetApp
July 05, 2024

Sommario

Utilizzare i comandi "sostituzione controller di sistema" per aggiornare l'hardware del controller introdotto in ONTAP 9.15.1

Panoramica

Questa procedura descrive come aggiornare l'hardware del controller utilizzando ARL (aggregate relocation) per le seguenti configurazioni di sistema:

Metodo	Versione di ONTAP	Sistemi supportati
Utilizzo di `system controller replace` comandi	9.15.1 o versione successiva	"Link alla matrice dei sistemi supportati"

Non è possibile utilizzare questa procedura per aggiornare una configurazione MetroCluster FC o IP. Per aggiornare una configurazione MetroCluster, consultare il "Riferimenti" collegamento alla *documentazione di aggiornamento ed espansione MetroCluster*.

Durante la procedura, l'hardware del controller originale viene aggiornato con l'hardware del controller sostitutivo, riallocando la proprietà degli aggregati non root. La migrazione degli aggregati viene eseguita più volte da un nodo all'altro per confermare che almeno un nodo fornisce i dati degli aggregati durante l'intera procedura di aggiornamento. Inoltre, è possibile migrare le interfacce logiche dei dati (LIF) e assegnare le porte di rete sul nuovo controller ai gruppi di interfacce durante la procedura.

Terminologia utilizzata in queste informazioni

In queste informazioni, i nodi originali sono chiamati "node1" e "node2", mentre i nuovi nodi sono chiamati "node3" e "node4". Durante la procedura descritta, il node1 viene sostituito dal node3, mentre il node2 viene sostituito dal node4.

I termini "node1", "node2", "node3" e "node4" vengono utilizzati solo per distinguere tra i nodi originali e quelli nuovi. Quando si segue la procedura, è necessario sostituire i nomi reali dei nodi originale e nuovo. Tuttavia, in realtà, i nomi dei nodi non cambiano: Node3 ha il nome node1 e node4 ha il nome node2 dopo l'aggiornamento dell'hardware del controller.

Informazioni importanti:

- Questa procedura è complessa e presuppone che si disponga di competenze di amministrazione avanzate di ONTAP. È inoltre necessario leggere e comprendere "Linee guida per l'aggiornamento dei controller con ARL" e a. "Panoramica dell'aggiornamento ARL" prima di iniziare l'aggiornamento.
- Questa procedura presuppone che l'hardware del controller sostitutivo sia nuovo e non sia stato utilizzato. I passaggi necessari per preparare i controller usati con il `wipeconfig` comando non sono inclusi in questa procedura. Se in precedenza è stato utilizzato l'hardware del controller sostitutivo, è necessario contattare il supporto tecnico.
- È possibile utilizzare questa procedura per aggiornare l'hardware del controller nei cluster con più di due nodi; tuttavia, è necessario eseguire la procedura separatamente per ogni coppia di ha (High Availability) nel cluster.
- Quando esegui l'upgrade a un sistema AFF A70, AFF A90 o AFF A1K introdotto in ONTAP 9.15.1, ONTAP converte l'efficienza dello storage di tutti i volumi con thin provisioning, inclusi quelli che non utilizzano l'efficienza dello storage e applica le nuove funzioni di efficienza dello storage che sfruttano la funzionalità

di offload dell'hardware. Si tratta di un processo in background automatico, senza alcun impatto visibile sulle prestazioni del sistema. "Scopri di più"

Automatizzare il processo di aggiornamento del controller

Durante un aggiornamento del controller, il controller viene sostituito con un altro controller che esegue una piattaforma più recente o più potente. Questo contenuto fornisce i passaggi per la procedura parzialmente automatizzata, che utilizza i controlli automatici di raggiungibilità delle porte di rete per semplificare ulteriormente l'esperienza di aggiornamento dei controller.

Decidere se utilizzare la procedura di trasferimento degli aggregati

Questa procedura descrive come aggiornare gli storage controller in una coppia ha con nuovi controller, mantenendo al contempo dati e dischi esistenti. Si tratta di una procedura complessa che deve essere utilizzata solo da amministratori esperti.

È possibile utilizzare questa procedura nelle seguenti circostanze:

- Si sta eseguendo ONTAP 9.15.1 o versione successiva.
- Non vuoi aggiungere i nuovi controller come nuova coppia ha al cluster e migrare i dati utilizzando la procedura di spostamento dei volumi.
- Si è esperti nell'amministrazione di ONTAP e si è a proprio agio con i rischi di lavorare in modalità diagnostica con privilegi.

Con questa procedura è possibile utilizzare NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) e NetApp aggregate Encryption (NAE).

Non è possibile utilizzare questa procedura nelle seguenti circostanze:

- Si sta eseguendo l'aggiornamento di AFF A800 a AFF A70 o AFF A90. Per eseguire questo aggiornamento di AFF A800, vedere "Riferimenti" il collegamento ai comandi *Use "System controller replace" (utilizza comando di sostituzione del controller di sistema) per aggiornare i modelli di controller nello stesso chassis*.
- Si sta aggiornando un sistema V-Series o un sistema di storage di virtualizzazione FlexArray utilizzando un array esterno per lo storage backend. Contattare il supporto tecnico per opzioni di aggiornamento di un sistema V-series o FlexArray.
- Si sta aggiornando una configurazione MetroCluster FC o IP. Per aggiornare una configurazione MetroCluster, consultare il "Riferimenti" collegamento alla *documentazione di aggiornamento ed espansione MetroCluster*.

la tabella seguente mostra la matrice di modelli supportata per l'aggiornamento del controller.

Controller esistente	Controller sostitutivo
AFF A300	AFF A70, AFF A90 e AFF A1K
AFF A400	AFF A70, AFF A90 e AFF A1K

Controller esistente	Controller sostitutivo
AFF A700	AFF A70, AFF A90 e AFF A1K
AFF A900	AFF A90 e AFF A1K

> AFF A70 e AFF A90 sono sistemi integrati con dischi integrati. I due controller e i dischi sono in un singolo chassis. Non è possibile aggiornare un sistema esistente se i nuovi controller dispongono di unità interne.
>
> Se la combinazione di modelli di upgrade del controller non è riportata nella tabella precedente, contattare il supporto tecnico.

Se si preferisce un metodo diverso per aggiornare l'hardware del controller e si desidera eseguire spostamenti di volume, fare riferimento a. "Riferimenti" Per collegarsi a *Upgrade spostando volumi o storage*.

Fare riferimento a. "Riferimenti" Collegamento al *Centro documentazione di ONTAP 9* da cui è possibile accedere alla documentazione del prodotto ONTAP 9.

Strumenti e documentazione richiesti

È necessario disporre di strumenti specifici per installare il nuovo hardware e consultare altri documenti durante il processo di aggiornamento.

Per eseguire l'aggiornamento sono necessari i seguenti strumenti:

- Cintura per la messa a terra
- Cacciavite Phillips n. 2

Accedere alla "Riferimenti" per accedere all'elenco dei documenti di riferimento e dei siti di riferimento necessari per questo aggiornamento

Linee guida per l'aggiornamento dei controller con ARL

Per capire se è possibile utilizzare ARL per aggiornare una coppia di controller con ONTAP 9.15.1 o versioni successive, dipende dalla piattaforma e dalla configurazione dei controller originali e di quelli sostitutivi.

Aggiornamenti supportati per ARL

Prima di aggiornare una coppia di nodi utilizzando questa procedura ARL, esaminare i seguenti requisiti per assicurarsi che la configurazione sia supportata:

- Verificare che l'ARL possa essere eseguito sulle unità di controllo originali e sostitutive.
- Verificare le dimensioni di tutti gli aggregati definiti e il numero di dischi supportati dal sistema originale. Quindi, occorre confrontare le dimensioni dell'aggregato e il numero di dischi supportati con le dimensioni dell'aggregato e il numero di dischi supportati dal nuovo sistema. Fare riferimento a "Riferimenti" per il collegamento a *Hardware Universe* dove sono disponibili queste informazioni. La dimensione aggregata e il numero di dischi supportati dal nuovo sistema devono essere uguali o superiori alla dimensione aggregata e al numero di dischi supportati dal sistema originale.

- Convalida nelle regole di miscelazione del cluster se i nuovi nodi possono diventare parte del cluster con i nodi esistenti quando viene sostituito il controller originale. Per ulteriori informazioni sulle regole di mescolamento dei cluster, fare riferimento al "Riferimenti" link al *Hardware Universe*.
- Migra e sposta nuovamente le LIF del cluster in due porte del cluster per nodo, se disponi di un sistema, ad esempio AFF 700, con la seguente configurazione:
- Più di due porte cluster per nodo
- Una scheda di interconnessione in cluster in slot4 in modalità breakout per creare porte e4a, e4b, e4c e E4D, e porte E4E, e4f, e4g e e4h

> L'aggiornamento del controller con più di due porte del cluster per nodo potrebbe causare la mancanza di LIF del cluster sul nuovo controller in seguito all'upgrade.

Per ulteriori informazioni, vedere l'articolo della Knowledge base "Come eliminare LIF del cluster indesiderate o non necessarie".

L'upgrade del controller tramite ARL è supportato sui sistemi configurati con volumi di conformità SnapLock Enterprise e SnapLock.

Cluster senza switch a due nodi

Se si stanno aggiornando i nodi in un cluster senza switch a due nodi, è possibile lasciare i nodi nel cluster senza switch durante l'aggiornamento. Non è necessario convertirli in un cluster con switch.

Aggiornamenti non supportati per ARL

Non puoi aggiornare i controller sostitutivi che non supportano gli shelf di dischi collegati ai controller originali.

Fare riferimento a. "Riferimenti" Per il collegamento a *Hardware Universe* per informazioni sul supporto dei dischi.

Se desideri aggiornare i controller entry-level con dischi interni, fai riferimento "Riferimenti" al link *Upgrade spostando volumi o storage* e accedi alla procedura *aggiornamento di una coppia di nodi in cui è in esecuzione Clustered Data ONTAP spostando volumi*.

Risolvere i problemi

Se si verificano problemi durante l'aggiornamento dei controller, consultare "Risolvere i problemi" per ulteriori informazioni e possibili soluzioni.

Se non si riesce a trovare una soluzione al problema riscontrato, contattare il supporto tecnico.

Panoramica dell'aggiornamento ARL

Prima di aggiornare i nodi utilizzando ARL, è necessario comprendere il funzionamento della procedura. In questo contenuto, la procedura viene suddivisa in diverse fasi.

Aggiornare la coppia di nodi

Per aggiornare la coppia di nodi, è necessario preparare i nodi originali ed eseguire una serie di passaggi sia sul nodo originale che su quello nuovo. È quindi possibile decommissionare i nodi originali.

Panoramica della sequenza di aggiornamento ARL

Durante la procedura, si aggiorna l'hardware del controller originale con l'hardware del controller sostitutivo, un controller alla volta, sfruttando la configurazione della coppia ha per trasferire la proprietà degli aggregati non root. Tutti gli aggregati non root devono essere sottoposti a due rilocazioni per raggiungere la destinazione finale, che è il nodo aggiornato corretto.

Ogni aggregato ha un proprietario di casa e un proprietario corrente. Il proprietario della casa è il proprietario effettivo dell'aggregato e il proprietario attuale è il proprietario temporaneo.

La seguente tabella descrive le attività di alto livello eseguite durante ciascuna fase e lo stato di proprietà aggregata alla fine della fase. Le fasi dettagliate vengono fornite più avanti nella procedura:

Fase	Descrizione
"Fase 1. Preparatevi per l'aggiornamento"	Durante la fase 1, vengono eseguiti controlli preliminari e, se necessario, vengono corretti i diritti di proprietà degli aggregati. È necessario registrare alcune informazioni se si gestisce la crittografia dello storage utilizzando OKM e si può scegliere di interrompere le relazioni di SnapMirror. Proprietà aggregata alla fine della fase 1: • Node1 è il proprietario della casa e l'attuale proprietario degli aggregati node1. • Node2 è il proprietario domestico e proprietario corrente degli aggregati node2.
"Fase 2. Spostare e dismettere il node1"	Durante la fase 2, è possibile spostare gli aggregati non root node1 e le LIF dei dati NAS in node2. Questo processo è in gran parte automatizzato; l'operazione viene interrotta per consentirti di controllarne lo stato. È necessario riprendere manualmente l'operazione. Se necessario, spostare gli aggregati non riusciti o vetoed. Prima di ritirare il node1, si registrano le informazioni node1 da utilizzare in seguito nella procedura. Puoi anche prepararti a netboot node3 e node4 più avanti nella procedura. Proprietà aggregata alla fine della fase 2: • Node2 è l'attuale proprietario degli aggregati node1. • Node2 è il proprietario domestico e proprietario corrente degli aggregati node2.

Fase	Descrizione
"Fase 3. Installazione e boot node3"	Durante la fase 3, si installa e si avvia node3, si controlla che il cluster e le porte di gestione dei nodi da node1 siano online sul node3 e si verifica l'installazione node3. Se si utilizza NetApp Volume Encryption (NVE), viene ripristinata la configurazione del gestore delle chiavi. È inoltre possibile spostare le LIF dei dati NAS node1 e gli aggregati non root da node2 a node3 e verificare che le LIF SAN esistano sul node3. Proprietà aggregata alla fine della fase 3: • Node3 è il proprietario della casa e il proprietario corrente degli aggregati node1. • Node2 è il proprietario domestico e proprietario corrente degli aggregati node2.
"Fase 4. Spostare e dismettere il node2"	Durante la fase 4, è possibile spostare aggregati non root e LIF dati NAS da node2 a node3. Inoltre, prima di ritirarlo, è possibile registrare le informazioni relative al nodo 2 da utilizzare in seguito nella procedura. Proprietà aggregata alla fine della fase 4: • Node3 è il proprietario della casa e l'attuale proprietario di aggregati che originariamente appartenevano al node1. • Node2 è il proprietario domestico degli aggregati node2. • Node3 è l'attuale proprietario degli aggregati node2.
"Fase 5. Installazione e boot node4"	Durante la fase 5, si installa e si avvia node4, si controlla che il cluster e le porte di gestione dei nodi da node2 siano online sul node4 e si verifica l'installazione node4. Se si utilizza NVE, si ripristina la configurazione del gestore delle chiavi. È inoltre possibile spostare le LIF dei dati NAS node2 e gli aggregati non root da node3 a node4 e verificare che le LIF SAN esistano sul node4. Proprietà aggregata alla fine della fase 5: • Node3 è il proprietario di casa e l'attuale proprietario degli aggregati che originariamente appartenevano al node1. • Node4 è il proprietario della casa e l'attuale proprietario di aggregati che originariamente appartenevano al node2.
"Fase 6. Completare l'aggiornamento"	Durante la fase 6, si conferma che i nuovi nodi sono impostati correttamente e, se i nuovi nodi sono abilitati per la crittografia, si configura e imposta Storage Encryption o NVE. È inoltre necessario decommissionare i vecchi nodi e riprendere le operazioni di SnapMirror.

Fase 1. Preparatevi per l’aggiornamento

Panoramica della fase 1

Durante la fase 1, vengono eseguiti controlli preliminari e, se necessario, vengono corretti i diritti di proprietà degli aggregati. È inoltre possibile registrare alcune informazioni se si gestisce la crittografia dello storage utilizzando Onboard Key Manager e scegliere di interrompere le relazioni di SnapMirror.

Fasi

1. "Preparare i nodi per l’aggiornamento"
2. "Gestire la crittografia dello storage utilizzando Onboard Key Manager"

Preparare i nodi per l’aggiornamento

Il processo di sostituzione del controller inizia con una serie di controlli preliminari. Si raccolgono inoltre informazioni sui nodi originali da utilizzare più avanti nella procedura e, se necessario, si determina il tipo di unità con crittografia automatica in uso.

Fasi

1. Iniziare il processo di sostituzione del controller immettendo il seguente comando nella riga di comando ONTAP:

   ```
   system controller replace start -nodes <node_names>
   ```

   > ⓘ È possibile eseguire il comando di avvio di sostituzione del controller di sistema solo al livello di privilegi avanzati: `set -privilege advanced`

   Viene visualizzato un output simile al seguente esempio. L’output mostra la versione di ONTAP in esecuzione sul cluster:

```
Warning: 1. Current ONTAP version is 9.15.1

2. Verify that NVMEM or NVRAM batteries of the new nodes are charged,
and charge them if they are not. You need to physically check the new
nodes to see if the NVMEM or NVRAM batteries are charged. You can check
the battery status either by connecting to a serial console or using
SSH, logging into the Service Processor (SP) or Baseboard Management
Controller (BMC) for your system, and use the system sensors to see if
the battery has a sufficient charge.

Attention: Do not try to clear the NVRAM contents. If there is a need to
clear the contents of NVRAM, contact NetApp technical support.

3. If a controller was previously part of a different cluster, run
wipeconfig before using it as the replacement controller.

4. Note: This is not a MetroCluster configuration. Controller
replacement supports only ARL based procedure.
Do you want to continue? {y|n}: y
```

2. Premere `y`, viene visualizzato il seguente output:

```
Controller replacement operation: Prechecks in progress.
Controller replacement operation has been paused for user intervention.
```

Il sistema esegue i seguenti controlli preliminari; registrare l'output di ogni controllo preliminare per l'utilizzo in seguito nella procedura:

Eseguire un controllo preliminare	Descrizione
Verifica dello stato del cluster	Controlla tutti i nodi del cluster per verificarne l'integrità.
Verifica dello stato di trasferimento aggregato	Verifica se è già in corso un trasferimento di aggregati. Se è in corso un altro trasferimento di aggregati, il controllo non riesce.
Controllo del nome del modello	Verifica se i modelli di controller sono supportati per questa procedura. Se i modelli non sono supportati, l'operazione non riesce.
Verifica del quorum del cluster	Verifica che i nodi da sostituire siano in quorum. Se i nodi non sono in quorum, l'attività non riesce.

Eseguire un controllo preliminare	Descrizione
Verifica della versione dell'immagine	Verifica che i nodi da sostituire eseguano la stessa versione di ONTAP. Se le versioni dell'immagine ONTAP sono diverse, l'operazione non riesce. Sui nuovi nodi deve essere installata la stessa versione di ONTAP 9.x installata sui nodi originali. Se nei nuovi nodi è installata una versione diversa di ONTAP, è necessario eseguire il netboot dei nuovi controller dopo averli installati. Per istruzioni su come aggiornare ONTAP, fare riferimento a. "Riferimenti" Collegamento a *Upgrade ONTAP*.
Verifica dello stato HA	Controlla se entrambi i nodi da sostituire sono in una configurazione di coppia ad alta disponibilità (ha). Se il failover dello storage non è abilitato per i controller, l'operazione non riesce.
Verifica dello stato dell'aggregato	Se i nodi che vengono sostituiti possiedono aggregati per i quali non sono proprietari di casa, l'attività non riesce. I nodi non devono possedere aggregati non locali.
Verifica dello stato del disco	Se i nodi da sostituire presentano dischi mancanti o guasti, l'attività non riesce. In caso di dischi mancanti, fare riferimento a. "Riferimenti" Per collegarsi a *Disk and aggregate management con CLI*, *Logical storage management con CLI* e *High Availability management* per configurare lo storage per la coppia ha.
Verifica dello stato LIF dei dati	Controlla se uno dei nodi da sostituire dispone di LIF di dati non locali. I nodi non devono contenere file di dati di cui non sono proprietari. Se uno dei nodi contiene LIF di dati non locali, l'attività non riesce.
Stato LIF del cluster	Verifica se le LIF del cluster sono in funzione per entrambi i nodi. Se le LIF del cluster non sono attive, l'attività non riesce.
Verifica dello stato ASUP	Se le notifiche ASUP non sono configurate, l'attività non riesce. È necessario attivare ASUP prima di iniziare la procedura di sostituzione del controller.
Verifica dell'utilizzo della CPU	Controlla se l'utilizzo della CPU è superiore al 50% per uno dei nodi da sostituire. Se l'utilizzo della CPU è superiore al 50% per un periodo di tempo considerevole, il task non riesce.
Controllo ricostruzione aggregata	Controlla se la ricostruzione avviene su qualsiasi aggregato di dati. Se la ricostruzione aggregata è in corso, l'operazione non riesce.
Verifica del processo di affinità del nodo	Controlla se sono in esecuzione lavori di affinità del nodo. Se i lavori di affinità del nodo sono in esecuzione, il controllo non riesce.

3. Una volta avviata l'operazione di sostituzione del controller e completate le verifiche preliminari, l'operazione viene interrotta e consente di raccogliere informazioni di output che potrebbero essere necessarie in seguito durante la configurazione del node3.

Prima di iniziare l'upgrade, dovrai migrare e ripristinare le LIF del cluster in due porte cluster per nodo, se disponi di un sistema come AFF 700, con la seguente configurazione:

- Più di due porte cluster per nodo
- Una scheda di interconnessione in cluster in slot4 in modalità breakout per creare porte e4a, e4b, e4c e E4D, e porte E4E, e4f, e4g e e4h

L'aggiornamento del controller con più di due porte del cluster per nodo potrebbe causare la mancanza di LIF del cluster sul nuovo controller in seguito all'upgrade.

Per ulteriori informazioni, vedere l'articolo della Knowledge base "Come eliminare LIF del cluster indesiderate o non necessarie".

4. Eseguire il seguente set di comandi come indicato dalla procedura di sostituzione del controller sulla console di sistema.

   Dalla porta seriale collegata a ciascun nodo, eseguire e salvare singolarmente l'output dei seguenti comandi:

   - `vserver services name-service dns show`
   - `network interface show -curr-node <local> -role <cluster,intercluster,node-mgmt,cluster-mgmt,data>`
   - `network port show -node <local> -type physical`
   - `service-processor show -node <local> -instance`
   - `network fcp adapter show -node <local>`
   - `network port ifgrp show -node <local>`
   - `system node show -instance -node <local>`
   - `run -node <local> sysconfig`
   - `storage aggregate show -r`
   - `storage aggregate show -node <local>`
   - `volume show -node <local>`
   - `system license show -owner <local>`
   - `storage encryption disk show`
   - `security key-manager onboard show-backup`
   - `security key-manager external show`
   - `security key-manager external show-status`
   - `network port reachability show -detail -node <local>`

   Se la crittografia del volume NetApp (NVE) o la crittografia aggregata NetApp (NAE) utilizzando il gestore delle chiavi integrato (OKM) è in uso, tenere la passphrase del gestore delle chiavi pronta per completare la risincronizzazione del gestore delle chiavi in un secondo momento della procedura.

5. Se il sistema utilizza dischi con crittografia automatica, consultare l'articolo della Knowledge base "Come verificare se un disco è certificato FIPS" Per determinare il tipo di unità con crittografia automatica in uso sulla coppia ha che si sta aggiornando. Il software ONTAP supporta due tipi di dischi con crittografia automatica:

   - Dischi SAS o NVMe NetApp Storage Encryption (NSE) certificati FIPS
   - Dischi NVMe con crittografia automatica non FIPS (SED)

   "Scopri di più sulle unità con crittografia automatica supportate".

Correggere la proprietà dell'aggregato se un controllo preliminare ARL non riesce

Se il controllo dello stato aggregato non riesce, è necessario restituire gli aggregati di proprietà del nodo partner al nodo proprietario domestico e avviare nuovamente il processo di pre-controllo.

Fasi

1. Restituire gli aggregati attualmente di proprietà del nodo partner al nodo home owner:

   `storage aggregate relocation start -node source_node -destination destination-node -aggregate-list *`

2. Verificare che né node1 né node2 possiedano ancora aggregati per i quali è il proprietario corrente (ma non il proprietario domestico):

   `storage aggregate show -nodes node_name -is-home false -fields owner-name, home-name, state`

   L'esempio seguente mostra l'output del comando quando un nodo è sia il proprietario corrente che il proprietario domestico degli aggregati:

```
cluster::> storage aggregate show -nodes node1 -is-home true -fields
owner-name,home-name,state
aggregate   home-name  owner-name  state
---------   ---------  ----------  ------
aggr1       node1      node1       online
aggr2       node1      node1       online
aggr3       node1      node1       online
aggr4       node1      node1       online

4 entries were displayed.
```

Al termine

È necessario riavviare il processo di sostituzione del controller:

`system controller replace start -nodes node_names`

Licenza

Per informazioni dettagliate sulle licenze ONTAP, fare riferimento a "Gestione delle licenze".

> L'utilizzo di funzioni senza licenza sul controller potrebbe mettere fuori conformità con il contratto di licenza.

Gestire la crittografia dello storage utilizzando Onboard Key Manager

È possibile utilizzare Onboard Key Manager (OKM) per gestire le chiavi di crittografia. Se si dispone di OKM configurato, è necessario registrare la passphrase e il materiale di backup prima di iniziare l'aggiornamento.

Fasi

1. Registrare la passphrase del cluster.

   Si tratta della passphrase immessa quando l'OKM è stato configurato o aggiornato utilizzando l'API CLI o REST.

2. Eseguire il backup delle informazioni del gestore delle chiavi eseguendo il `security key-manager onboard show-backup` comando.

Interrompere le relazioni di SnapMirror (facoltativo)

Prima di continuare con la procedura, è necessario confermare che tutte le relazioni di SnapMirror siano interrotti. Quando una relazione SnapMirror viene ritirata, rimane irreparata in caso di riavvii e failover.

Fasi

1. Verificare lo stato della relazione SnapMirror sul cluster di destinazione:

   ```
   snapmirror show
   ```

   > Se lo stato è "trasferimento", è necessario interrompere questi trasferimenti: `snapmirror abort -destination-vserver` *`vserver_name`*

   L'interruzione non riesce se la relazione SnapMirror non si trova nello stato di "trasferimento".

2. Interrompere tutte le relazioni tra il cluster:

   ```
   snapmirror quiesce -destination-vserver *
   ```

Fase 2. Spostare e dismettere il node1

Panoramica della fase 2

Durante la fase 2, è possibile spostare gli aggregati non root node1 e le LIF dei dati NAS in node2. Questo processo è in gran parte automatizzato; l'operazione viene interrotta per consentirti di controllarne lo stato. È necessario riprendere manualmente l'operazione. Se necessario, spostare gli aggregati non riusciti o vetoed. Inoltre,

registrare le informazioni necessarie sul node1, dismettere il node1 e prepararsi al netboot node3 e node4 più avanti nella procedura.

Fasi

1. "Spostare gli aggregati non root e le LIF dei dati NAS di proprietà del node1 al node2"
2. "Spostare gli aggregati non riusciti o vetoed"
3. "Ritirare il node1"
4. "Preparatevi per il netboot"

Spostare gli aggregati non root e le LIF dei dati NAS di proprietà del node1 al node2

Prima di poter sostituire il node1 con il node3, è necessario spostare gli aggregati non root e le LIF dei dati NAS da node1 a node2 prima di spostare le risorse del node1 al node3.

Prima di iniziare

L'operazione dovrebbe essere già in pausa quando si inizia l'operazione; è necessario ripristinarla manualmente.

A proposito di questa attività

Una volta migrati gli aggregati e i LIF, l'operazione viene sospesa per scopi di verifica. In questa fase, è necessario verificare se tutti gli aggregati non root e le LIF di dati non SAN vengono migrati in node3.

> Il proprietario domestico degli aggregati e dei LIF non viene modificato; viene modificato solo il proprietario corrente.

Fasi

1. Riprendere le operazioni di trasferimento aggregato e spostamento LIF dei dati NAS:

   ```
   system controller replace resume
   ```

   Tutti gli aggregati non root e le LIF dei dati NAS vengono migrati da node1 a node2.

   L'operazione viene interrotta per consentire di verificare se tutti gli aggregati non root e le LIF di dati non SAN node1 sono stati migrati in node2.

2. Controllare lo stato delle operazioni di trasferimento aggregato e LIF dei dati NAS:

   ```
   system controller replace show-details
   ```

3. Con l'operazione ancora in pausa, verificare che tutti gli aggregati non root siano in linea per il loro stato su node2:

   ```
   storage aggregate show -node node2 -state online -root false
   ```

   L'esempio seguente mostra che gli aggregati non root su node2 sono online:

```
cluster::> storage aggregate show -node node2 state online -root false

Aggregate  Size     Available  Used%  State  #Vols  Nodes  RAID Status
---------  -------  ---------  -----  ------ -----  ------
--------------
aggr_1     744.9GB  744.8GB    0%     online     5  node2
raid_dp,normal
aggr_2     825.0GB  825.0GB    0%     online     1  node2
raid_dp,normal
2 entries were displayed.
```

Se gli aggregati sono andati offline o diventano estranei sul node2, portarli online usando il seguente comando su node2, una volta per ogni aggregato:

`storage aggregate online -aggregate` *`aggr_name`*

4. Verificare che tutti i volumi siano online sul nodo 2 utilizzando il seguente comando sul nodo 2 ed esaminandone l'output:

   `volume show -node` *`node2`* `-state offline`

   Se alcuni volumi sono offline sul nodo 2, portarli online utilizzando il seguente comando sul nodo 2, una volta per ogni volume:

   `volume online -vserver` *`vserver_name`* `-volume` *`volume_name`*

   Il *`vserver_name`* da utilizzare con questo comando si trova nell'output del precedente `volume show` comando.

5. se i LIF non sono attivi, impostare lo stato amministrativo dei LIF su `up` Utilizzando il seguente comando, una volta per ogni LIF:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-home-node` *`nodename`* `-status-admin up`

Spostare gli aggregati non riusciti o vetoed

Se gli aggregati non vengono ricollocati o vengono vetoati, è necessario riallocarli manualmente o, se necessario, eseguire l'override dei veti o dei controlli di destinazione.

A proposito di questa attività

L'operazione di riposizionamento sarà stata sospesa a causa dell'errore.

Fasi

1. Controllare i registri del sistema di gestione degli eventi (EMS) per determinare il motivo per cui l'aggregato non è stato riallocato o è stato vetoed.
2. Spostare eventuali aggregati guasti o vetoed:

   `storage aggregate relocation start -node` *`node1`* `-destination` *`node2`* `-aggregate`

```
-list aggr_name -ndo-controller-upgrade true
```

3. Quando richiesto, immettere `y`.
4. È possibile forzare il trasferimento utilizzando uno dei seguenti metodi:

Opzione	Descrizione
Ignorare i controlli di veto	Utilizzare il seguente comando: `storage aggregate relocation start -node node1 -destination node2 -aggregate-list aggr_list -ndo -controller-upgrade true -override-vetoes true`
Ignorare i controlli di destinazione	Utilizzare il seguente comando: `storage aggregate relocation start -node node1 -destination node2 -aggregate-list aggr_list -ndo -controller-upgrade true -override-vetoes true -override-destination-checks true`

Ritirare il node1

Per dismettere il node1, riprendere l'operazione automatica per disattivare correttamente la coppia ha con node2 e chiudere node1. Più avanti nella procedura, rimuovere il nodo 1 dal rack o dallo chassis.

Fasi

1. Riprendere l'operazione:

```
system controller replace resume
```

2. Verificare che il node1 sia stato arrestato:

```
system controller replace show-details
```

Al termine

Una volta completato l'aggiornamento, è possibile decommissionare il node1. Vedere "Decommissionare il vecchio sistema".

Preparatevi per il netboot

Dopo aver inserito fisicamente il nodo 3 e il nodo 4 più avanti nella procedura, potrebbe essere necessario eseguire il netboot. Il termine "netboot" indica che si sta eseguendo l'avvio da un'immagine ONTAP memorizzata su un server remoto. Quando ci si prepara per il netboot, si inserisce una copia dell'immagine di boot di ONTAP 9 su un server web a cui il sistema può accedere.

È anche possibile utilizzare l'opzione di avvio USB per eseguire un netboot. Consultare l'articolo della Knowledge base "Come utilizzare il comando boot_recovery LOADER per installare ONTAP per la configurazione iniziale di un sistema".

Prima di iniziare

- Verificare che sia possibile accedere a un server HTTP con il sistema.
- Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp* e scaricare i file di sistema necessari per la piattaforma e la versione corretta di ONTAP.

A proposito di questa attività

È necessario eseguire il netboot dei nuovi controller se non sono installati sulla stessa versione di ONTAP 9 installata sui controller originali. Dopo aver installato ciascun nuovo controller, avviare il sistema dall'immagine di ONTAP 9 memorizzata sul server Web. È quindi possibile scaricare i file corretti sul dispositivo di avvio per i successivi avvii del sistema.

Fasi

1. Accedere al NetApp Support Site per scaricare i file utilizzati per eseguire l'avvio da rete del sistema.
2. Scaricare il software ONTAP appropriato dalla sezione di download del software del sito di supporto NetApp e memorizzare il `<ontap_version>_image.tgz` file in una directory accessibile dal web.
3. Passare alla directory accessibile dal Web e verificare che i file necessari siano disponibili.

   L'elenco delle directory deve contenere il seguente file:
   `<ontap_version>_image.tgz`

   > Non è necessario estrarre il contenuto di `<ontap_version>_image.tgz` file.

   Verranno utilizzate le informazioni contenute nelle directory in "Fase 3".

Fase 3. Installazione e boot node3

Panoramica della fase 3

Durante la fase 3, si installa e si avvia node3, si controlla che il cluster e le porte di gestione dei nodi da node1 siano online sul node3 e si verifica l'installazione node3. Se si utilizza NetApp Volume Encryption (NVE), viene ripristinata la configurazione del gestore delle chiavi. È inoltre possibile spostare le LIF dei dati NAS node1 e gli aggregati non root da node2 a node3 e verificare che le LIF SAN esistano sul node3.

Fasi

1. "Installazione e boot node3"
2. "Verificare l'installazione di node3"
3. "Ripristinare la configurazione del gestore delle chiavi sul node3"
4. "Spostare gli aggregati non root e le LIF di dati NAS di proprietà del node1 da node2 a node3"

Installazione e boot node3

Si installa node3 nel rack, si trasferiscono le connessioni node1 a node3, si avvia node3 e si installa ONTAP. È quindi necessario riassegnare i dischi di riserva di node1, gli eventuali dischi appartenenti al volume root e gli eventuali aggregati non root che non sono stati ricollocati a node2 nelle fasi precedenti del processo, come descritto in questa sezione.

A proposito di questa attività

L'operazione di trasferimento viene messa in pausa all'inizio di questa fase. Questo processo è in gran parte automatizzato; l'operazione viene interrotta per consentirti di controllarne lo stato. È necessario riprendere manualmente l'operazione. Inoltre, occorre verificare che le LIF SAN siano online e assegnate alle porte fisiche FC corrette sulla node3.

È necessario eseguire il netboot node3 se non dispone della stessa versione di ONTAP 9 installata sul node1. Dopo aver installato node3, avviarlo dall'immagine di ONTAP 9 memorizzata sul server Web. È quindi possibile scaricare i file corretti sul dispositivo di avvio per i successivi avviamenti del sistema, seguendo le istruzioni riportate in "Preparatevi per il netboot".

Fasi

1. assicurarsi di disporre di spazio rack per node3.

   I requisiti di spazio e altezza per i nuovi nodi potrebbero essere diversi dai nodi esistenti. Pianificare i requisiti di spazio per lo scenario di aggiornamento.

2. installare node3 nel rack, seguendo le *istruzioni di installazione e configurazione* per il modello di nodo in uso.
3. cavo node3, spostamento delle connessioni da node1 a node3.

   A partire da ONTAP 9.15.1, i nuovi modelli di controller dispongono di una sola porta "chiave" per il controller BMC (Baseboard Management Controller) e le connessioni di gestione. Pianificare le modifiche del cablaggio di conseguenza.

   - Console (porta di gestione remota)
   - Porte ha e cluster
   - Porte dati
   - Porte di gestione di cluster e nodi
   - Porte di storage Ethernet e SAS (Serial-Attached SCSI)
   - Configurazioni SAN: Porte switch iSCSI Ethernet, FC e NVMe/FC

   Potrebbe essere necessario sostituire i cavi di interconnessione tra i controller vecchi e nuovi per consentire l'interoperabilità tra i diversi modelli di controller e di schede. Per una mappa dei cablaggi degli shelf di storage Ethernet dei sistemi in uso, fare riferimento alla "procedure di installazione del sistema" .

   Per i controller introdotti in ONTAP 9.15.1 e versioni successive, il cluster e le interconnessioni ha utilizzano le stesse porte. Per le configurazioni con connessione da switch, è necessario collegare porte simili agli stessi switch del cluster. Ad esempio, quando si esegue l'upgrade a AFF A1K da un controller esistente, è necessario collegare E1a porte su entrambi i nodi a uno switch e e7a porte su entrambi i nodi al secondo switch.

4. accendere il computer in node3, quindi interrompere il processo di boot premendo Ctrl-C sul terminale della console per accedere al prompt dell'ambiente di boot.

   Quando si avvia node3, potrebbe essere visualizzato il seguente messaggio di avviso:

```
WARNING: The battery is unfit to retain data during a power outage. This
is likely because the battery is discharged but could be due to other
temporary conditions.
When the battery is ready, the boot process will complete and services
will be engaged.
To override this delay, press 'c' followed by 'Enter'
```

5. se viene visualizzato il messaggio di avviso in Fase 4, eseguire le seguenti operazioni:

   a. Verificare la presenza di eventuali messaggi della console che potrebbero indicare un problema diverso da una batteria NVRAM in esaurimento e, se necessario, intraprendere le azioni correttive necessarie.

   b. Attendere che la batteria si ricarichi e che il processo di avvio venga completato.

   Attenzione: Non ignorare il ritardo; il mancato caricamento della batteria potrebbe causare la perdita di dati.

   Fare riferimento a. "Preparatevi per il netboot".

6. configurare la connessione netboot scegliendo una delle seguenti operazioni.

   È necessario utilizzare la porta di gestione e l'IP come connessione di netboot. Non utilizzare un IP LIF dei dati, altrimenti potrebbe verificarsi un'interruzione dei dati durante l'aggiornamento.

Se DHCP (Dynamic host Configuration Protocol) è…	**Quindi…**
In esecuzione	Configurare la connessione automaticamente utilizzando il seguente comando al prompt dell'ambiente di boot: `ifconfig e0M -auto`
Non in esecuzione	Configurare manualmente la connessione utilizzando il seguente comando al prompt dell'ambiente di boot: `ifconfig e0M -addr=`*`filer_addr`* `-mask=`*`netmask`* `-gw=`*`gateway`* `-dns=`*`dns_addr`* `-domain=`*`dns_domain`* *`filer_addr`* È l'indirizzo IP del sistema di storage (obbligatorio). *`netmask`* è la maschera di rete del sistema di storage (obbligatoria). *`gateway`* è il gateway per il sistema storage (obbligatorio). *`dns_addr`* È l'indirizzo IP di un name server sulla rete (opzionale). *`dns_domain`* È il nome di dominio DNS (Domain Name Service) (facoltativo). Potrebbero essere necessari altri parametri per l'interfaccia. Invio `help ifconfig` al prompt del firmware per ulteriori informazioni.

7. Esegui netboot al nodo3:

   ```
   netboot http://<web_server_ip/path_to_web-
   accessible_directory>/<ontap_version>_image.tgz
   ```

   Il `<path_to_the_web-accessible_directory>` dovrebbe portare alla posizione in cui è stato scaricato `<ontap_version>_image.tgz` nella sezione "Preparatevi per il netboot".

   > Non interrompere l'avvio.

8. dal menu di boot, selezionare l'opzione `(7) Install new software first`.

   Questa opzione di menu consente di scaricare e installare la nuova immagine ONTAP sul dispositivo di avvio.

   Ignorare il seguente messaggio:

   ```
   This procedure is not supported for Non-Disruptive Upgrade on an HA pair
   ```

   La nota si applica agli aggiornamenti senza interruzioni di ONTAP e non agli aggiornamenti dei controller.

   > Utilizzare sempre netboot per aggiornare il nuovo nodo all'immagine desiderata. Se si utilizza un altro metodo per installare l'immagine sul nuovo controller, l'immagine potrebbe non essere corretta. Questo problema riguarda tutte le versioni di ONTAP. La procedura di netboot combinata con l'opzione `(7) Install new software` Consente di cancellare il supporto di avvio e di posizionare la stessa versione di ONTAP su entrambe le partizioni dell'immagine.

9. se viene richiesto di continuare la procedura, immettere `y`E quando viene richiesto il pacchetto, immettere l'URL:

   ```
   http://<web_server_ip/path_to_web-
   accessible_directory>/<ontap_version>_image.tgz
   ```

10. completare i seguenti passaggi secondari per riavviare il modulo controller:

    a. Invio `n` per ignorare il ripristino del backup quando viene visualizzato il seguente prompt:

       ```
       Do you want to restore the backup configuration now? {y|n}
       ```

    b. Invio `y` per riavviare quando viene visualizzato il seguente prompt:

       ```
       The node must be rebooted to start using the newly installed software. Do
       you want to reboot now? {y|n}
       ```

    Il modulo controller si riavvia ma si arresta al menu di avvio perché il dispositivo di avvio è stato riformattato e i dati di configurazione devono essere ripristinati.

11. selezionare la modalità di manutenzione `5` dal menu di boot e premere `y` quando viene richiesto di continuare con l'avvio.
12. verificare che il controller e lo chassis siano configurati come ha:

```
ha-config show
```

L'esempio seguente mostra l'output di `ha-config show` comando:

```
Chassis HA configuration: ha
Controller HA configuration: ha
```

Il sistema registra in una PROM sia che si trovi in una coppia ha o in una configurazione standalone. Lo stato deve essere lo stesso su tutti i componenti all'interno del sistema standalone o della coppia ha.

13. Se il controller e lo chassis non sono configurati come ha, utilizzare i seguenti comandi per correggere la configurazione:

```
ha-config modify controller ha

ha-config modify chassis ha
```

14. Verificare che tutte le porte Ethernet utilizzate per il collegamento agli shelf Ethernet siano configurate come storage:

```
storage port show
```

L'output visualizzato dipende dalla configurazione del sistema. Il seguente esempio di uscita si riferisce a un nodo con una singola scheda di memoria in slot11. L'output del sistema potrebbe essere diverso:

```
*> storage port show
Port Type Mode    Speed(Gb/s) State    Status  VLAN ID
---- ---- ------- ----------- -------- ------- -------
e11a ENET storage 100 Gb/s    enabled  online  30
e11b ENET storage 100 Gb/s    enabled  online  30
```

15. Modificare le porte non impostate per la memorizzazione:

```
storage port modify -p <port> -m storage
```

Tutte le porte Ethernet collegate agli shelf di storage devono essere configurate come storage per consentire l'accesso ai dischi e agli shelf.

16. Uscire dalla modalità di manutenzione:

```
halt
```

Interrompere l'autoboot premendo `Ctrl-C` al prompt dell'ambiente di boot.

17. Al nodo 2, controllare la data, l'ora e il fuso orario del sistema:

```
date
```

18. Su node3, controllare la data utilizzando il seguente comando al prompt dell'ambiente di avvio:

    `show date`

19. Se necessario, impostare la data sul node3:

    `set date <mm/dd/yyyy>`

20. In node3, controllare l'ora utilizzando il seguente comando al prompt dell'ambiente di boot:

    `show time`

21. Se necessario, impostare l'ora su node3:

    `set time <hh:mm:ss>`

22. Nel boot loader, impostare l'ID del sistema partner su node3:

    `setenv partner-sysid <node2_sysid>`

    Per il nodo 3, `partner-sysid` deve essere quello del node2.

    a. Salvare le impostazioni:

       `saveenv`

23. verificare `partner-sysid` per il nodo 3:

    `printenv partner-sysid`

24. Se si dispone di unità NetApp Storage Encryption (NSE) installate, attenersi alla seguente procedura.

    Se la procedura non è stata ancora eseguita, consultare l'articolo della Knowledge base "Come verificare se un disco è certificato FIPS" per determinare il tipo di unità con crittografia automatica in uso.

    a. Impostare `bootarg.storageencryption.support` a. `true` oppure `false`:

Se i seguenti dischi sono in uso…	**Quindi…**
Unità NSE conformi ai requisiti di crittografia automatica FIPS 140-2 livello 2	`setenv bootarg.storageencryption.support` **`true`**
SED non FIPS di NetApp	`setenv bootarg.storageencryption.support` **`false`**

    b. Accedere al menu di avvio speciale e selezionare l'opzione `(10) Set Onboard Key Manager recovery secrets`.

       Inserire la passphrase e le informazioni di backup registrate in precedenza. Vedere "Gestire la crittografia dello storage utilizzando Onboard Key Manager".

25. Nodo di boot nel menu di boot:

    ```
    boot_ontap menu
    ```

26. Su node3, andare al menu di avvio e utilizzando 22/7, selezionare l'opzione nascosta `boot_after_controller_replacement`. Al prompt, immettere node1 per riassegnare i dischi di node1 a node3, come nell'esempio seguente.

Espandere l'esempio di output della console

```
LOADER-A> boot_ontap menu
.
<output truncated>
.
All rights reserved.
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
.
<output truncated>
.
Please choose one of the following:
(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 22/7
(22/7) Print this secret List
(25/6) Force boot with multiple filesystem disks missing.
(25/7) Boot w/ disk labels forced to clean.
(29/7) Bypass media errors.
(44/4a) Zero disks if needed and create new flexible root volume.
(44/7) Assign all disks, Initialize all disks as SPARE, write DDR
labels
.
<output truncated>
.
(wipeconfig)                        Clean all configuration on boot
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
```

```
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.
The boot device has changed. System configuration information could
be lost. Use option (6) to restore the system configuration, or
option (4) to initialize all disks and setup a new system.
Normal Boot is prohibited.
Please choose one of the following:
(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? boot_after_controller_replacement
This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes
.
<output truncated>
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
<output truncated>
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
```

```
<node reboots>
System rebooting...
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
<output truncated>
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
Login:
```

Nell'esempio di output della console precedente, ONTAP richiederà il nome del nodo partner se il sistema utilizza dischi di partizione avanzata dei dischi (ADP).

27. Se il sistema entra in un ciclo di riavvio con il messaggio `no disks found`, indica che si è verificato un problema con la riassegnazione del disco. Consultare "Risolvere i problemi" per risolvere il problema.
28. Premere `Ctrl-C` durante l'operazione di autoboot per arrestare il nodo al `LOADER>` prompt.
29. Al prompt del CARICATORE, accedere alla modalità di manutenzione:

    ```
    boot_ontap maint
    ```

30. Verificare connettività del disco, stringa del modello del controller, configurazione ha e altri dettagli relativi alla connettività hardware.
31. Uscire dalla modalità di manutenzione:

    ```
    halt
    ```

32. al prompt del CARICATORE, avviare:

    ```
    boot_ontap menu
    ```

    Ora, all'avvio, il nodo è in grado di rilevare tutti i dischi ad esso assegnati in precedenza e di avviarsi come previsto.

    Quando i nodi del cluster che si stanno sostituendo utilizzano la crittografia dei volumi root, ONTAP non è in grado di leggere le informazioni sul volume dai dischi. Ripristinare le chiavi del volume root.

    Ciò si applica solo quando il volume principale utilizza la crittografia dei volumi di NetApp.

    a. Tornare al menu di avvio speciale:

```
LOADER> boot_ontap menu
```

```
Please choose one of the following:
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.

Selection (1-11)? 10
```

b. Selezionare **(10) Imposta segreti di ripristino di Onboard Key Manager**

c. Invio `y` al seguente prompt:

```
This option must be used only in disaster recovery procedures. Are you sure?
(y or n): y
```

d. Quando richiesto, inserire la passphrase del gestore delle chiavi.

e. Inserire i dati di backup quando richiesto.

> È necessario aver ottenuto la passphrase e i dati di backup in "Preparare i nodi per l'aggiornamento" sezione di questa procedura.

f. Dopo aver riavviato il sistema con lo speciale menu di boot, eseguire l'opzione **(1) Avvio normale**

> In questa fase potrebbe verificarsi un errore. Se si verifica un errore, ripetere i passaggi secondari in Passaggio 32 fino a quando il sistema non si avvia normalmente.

Verificare l'installazione di node3

È necessario verificare che le porte fisiche dal nodo 1 siano mappate correttamente alle porte fisiche sul nodo 3. In questo modo, il nodo 3 potrà comunicare con altri nodi del cluster e con la rete dopo l'aggiornamento.

A proposito di questa attività

Fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe* per acquisire informazioni sulle porte sui nuovi nodi. Le informazioni verranno utilizzate più avanti in questa sezione.

Il layout fisico delle porte potrebbe variare a seconda del modello dei nodi. All'avvio del nuovo nodo, ONTAP tenterà di determinare quali porte dovrebbero ospitare le LIF del cluster per entrare automaticamente nel quorum.

Se le porte fisiche sul nodo 1 non vengono mappate direttamente alle porte fisiche sul nodo 3, consultare la sezione successiva Ripristinare la configurazione di rete sul nodo 3 deve essere utilizzato per riparare la connettività di rete.

Dopo aver installato e avviato il nodo 3, è necessario verificare che sia installato correttamente. È necessario attendere che il nodo 3 si unisca al quorum e riprendere l'operazione di trasferimento.

A questo punto della procedura, l'operazione verrà messa in pausa quando node3 si unisce al quorum.

Fasi

1. Verificare che node3 si sia Unito al quorum:

   ```
   cluster show -node node3 -fields health
   ```

   L'output di `health` il campo deve essere `true`.

2. Verificare che node3 faccia parte dello stesso cluster di node2 e che sia integro:

   ```
   cluster show
   ```

3. passare alla modalità privilegi avanzati:

   ```
   set advanced
   ```

4. Controllare lo stato dell'operazione di sostituzione del controller e verificare che sia in stato di pausa e nello stesso stato in cui si trovava prima dell'arresto del node1 per eseguire le attività fisiche di installazione di nuovi controller e cavi in movimento:

   ```
   system controller replace show
   ```

   ```
   system controller replace show-details
   ```

5. Riprendere l'operazione di sostituzione del controller:

   ```
   system controller replace resume
   ```

6. La sostituzione del controller viene interrotta per l'intervento con il seguente messaggio:

```
Cluster::*> system controller replace show
Node             Status                        Error-Action
---------------- ------------------------
-----------------------------------
Node1(now node3) Paused-for-intervention      Follow the instructions
given in
                                               Step Details
Node2                       None

Step Details:
-------------------------------------------
To complete the Network Reachability task, the ONTAP network
configuration must be manually adjusted to match the new physical
network configuration of the hardware. This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For
detailed commands and instructions, refer to the "Re-creating VLANs,
ifgrps, and broadcast domains" section of the upgrade controller
hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement network displaced-vlans restore" to restore the VLAN on the
desired port.

2 entries were displayed.
```

In questa procedura, la sezione *creazione di VLAN, ifgrps e domini di trasmissione* è stata rinominata *Ripristino configurazione di rete su node3*.

7. Con la sostituzione del controller in stato di pausa, passare alla sezione successiva di questo documento per ripristinare la configurazione di rete sul nodo.

Ripristinare la configurazione di rete sul nodo 3

Dopo aver confermato che node3 è in quorum e può comunicare con node2, verificare che le VLAN, i gruppi di interfacce e i domini di broadcast di node1 siano visibili sul node3. Inoltre, verificare che tutte le porte di rete node3 siano configurate nei rispettivi domini di trasmissione corretti.

A proposito di questa attività

Per ulteriori informazioni sulla creazione e la ricreazione di VLAN, gruppi di interfacce e domini di trasmissione, fare riferimento a. "Riferimenti" Per collegarsi a *Network Management*.

Fasi

1. Elenca tutte le porte fisiche su cui è stato eseguito l'upgrade node1 (indicate come node3):

```
network port show -node node3
```

Vengono visualizzate tutte le porte di rete fisiche, le porte VLAN e le porte del gruppo di interfacce sul nodo. Da questo output, è possibile visualizzare le porte fisiche spostate in `Cluster` Dominio di broadcast di ONTAP. È possibile utilizzare questo output per agevolare la scelta delle porte da utilizzare come porte membro del gruppo di interfacce, porte di base VLAN o porte fisiche standalone per l'hosting di LIF.

2. Elencare i domini di broadcast sul cluster:

   `network port broadcast-domain show`

3. Elencare la raggiungibilità della porta di rete di tutte le porte su node3:

   `network port reachability show`

   L'output dovrebbe essere simile al seguente esempio:

```
ClusterA::*> network port reachability show
Node      Port     Expected Reachability               Reachability
Status
--------- -------- ----------------------------------
---------------------
node1_node3
          e0M      Default:Mgmt                       ok
          e10a     Default:Default                    ok
          e10b     -                                  no-reachability
          e10c     Default:Default                    ok
          e10d     -                                  no-reachability
          e1a      Cluster:Cluster                    ok
          e1b      -                                  no-reachability
          e7a      Cluster:Cluster                    ok
          e7b      -                                  no-reachability
node2_node4
          e0M      Default:Mgmt                       ok
          e4a      Default:Default                    ok
          e4b      -                                  no-reachability
          e4c      Default:Default                    ok
          e4d      -                                  no-reachability
          e3a      Cluster:Cluster                    ok
          e3b      Cluster:Cluster                    ok
18 entries were displayed.
```

   Nell'esempio precedente, node1_node3 viene appena avviato dopo la sostituzione del controller. Alcune porte non sono raggiungibili per i domini di trasmissione previsti e devono essere riparate.

4. Ripristina la raggiungibilità per ciascuna delle porte su node3 con uno stato di raggiungibilità diverso da `ok`. Eseguire il seguente comando, prima su qualsiasi porta fisica, quindi su qualsiasi porta VLAN, una alla volta:

   `network port reachability repair -node <node_name> -port <port_name>`

L'output dovrebbe essere simile al seguente esempio:

```
Cluster ::> reachability repair -node node1_node3 -port e4a
```

```
Warning: Repairing port "node1_node3: e4a" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

Un messaggio di avviso, come mostrato sopra, è previsto per le porte con uno stato di raggiungibilità che potrebbe essere diverso dallo stato di raggiungibilità del dominio di trasmissione in cui si trova attualmente. Esaminare la connettività della porta e rispondere `y` oppure `n` a seconda dei casi.

Verificare che tutte le porte fisiche abbiano la raggiungibilità prevista:

```
network port reachability show
```

Quando viene eseguita la riparazione della raggiungibilità, ONTAP tenta di posizionare le porte nei domini di trasmissione corretti. Tuttavia, se non è possibile determinare la raggiungibilità di una porta e non appartiene a nessuno dei domini di broadcast esistenti, ONTAP creerà nuovi domini di broadcast per queste porte.

5. Se la configurazione del gruppo di interfacce non corrisponde al layout della porta fisica del nuovo controller, modificarla seguendo la procedura riportata di seguito.

   a. È necessario innanzitutto rimuovere le porte fisiche che devono essere porte membro del gruppo di interfacce dall'appartenenza al dominio di trasmissione. Per eseguire questa operazione, utilizzare il seguente comando:

      ```
      network port broadcast-domain remove-ports -broadcast-domain <broadcast-
      domain_name> -ports <node_name:port_name>
      ```

   b. Aggiungere una porta membro a un gruppo di interfacce:

      ```
      network port ifgrp add-port -node <node_name> -ifgrp <ifgrp> -port
      <port_name>
      ```

   c. Il gruppo di interfacce viene aggiunto automaticamente al dominio di trasmissione circa un minuto dopo l'aggiunta della prima porta membro.

   d. Verificare che il gruppo di interfacce sia stato aggiunto al dominio di trasmissione appropriato:

      ```
      network port reachability show -node <node_name> -port <ifgrp>
      ```

      Se lo stato di raggiungibilità del gruppo di interfacce non è `ok`, assegnarlo al dominio di trasmissione appropriato:

```
network port broadcast-domain add-ports -broadcast-domain
<broadcast_domain_name> -ports <node:port>
```

6. Assegnare le porte fisiche appropriate al dominio di broadcast attenendosi alla `Cluster` seguente procedura:

a. Determinare quali porte hanno la raggiungibilità di `Cluster` dominio di broadcast:

```
network port reachability show -reachable-broadcast-domains Cluster:Cluster
```

b. Riparare qualsiasi porta con la possibilità di accedere a `Cluster` dominio di broadcast, se il suo stato di raggiungibilità non è `ok`:

```
network port reachability repair -node <node_name> -port <port_name>
```

7. Spostare le restanti porte fisiche nei domini di trasmissione corretti utilizzando uno dei seguenti comandi:

```
network port reachability repair -node <node_name> -port <port_name>
```

```
network port broadcast-domain remove-port
```

```
network port broadcast-domain add-port
```

Verificare che non siano presenti porte irraggiungibili o impreviste. Verificare lo stato di raggiungibilità di tutte le porte fisiche utilizzando il comando seguente ed esaminare l'output per confermare lo stato `ok`:

```
network port reachability show -detail
```

8. Ripristinare eventuali VLAN che potrebbero essere state spostate seguendo la procedura riportata di seguito:

a. Elenco VLAN spostate:

```
cluster controller-replacement network displaced-vlans show
```

Viene visualizzato un output simile al seguente:

```
Cluster::*> displaced-vlans show
(cluster controller-replacement network displaced-vlans show)
          Original
Node      Base Port   VLANs
--------  ----------  ----------------------------------------
Node1       a0a       822, 823
            e4a       822, 823
2 entries were displayed.
```

b. Ripristinare le VLAN spostate dalle porte di base precedenti:

```
cluster controller-replacement network displaced-vlans restore
```

Di seguito viene riportato un esempio di ripristino delle VLAN spostate dal gruppo di interfacce "a0a" allo stesso gruppo di interfacce:

```
Cluster::*> displaced-vlans restore -node node1_node3 -port a0a
-destination-port a0a
```

Di seguito viene riportato un esempio di ripristino delle VLAN spostate sulla porta "e9a" in "e9d":

```
Cluster::*> displaced-vlans restore -node node1_node3 -port e9a
-destination-port e9d
```

Quando un ripristino della VLAN ha esito positivo, le VLAN spostate vengono create sulla porta di destinazione specificata. Il ripristino della VLAN non riesce se la porta di destinazione è membro di un gruppo di interfacce o se la porta di destinazione non è disponibile.

Attendere circa un minuto per inserire le VLAN appena ripristinate nei domini di trasmissione appropriati.

a. Creare nuove porte VLAN in base alle necessità per le porte VLAN non presenti in `cluster controller-replacement network displaced-vlans show` ma deve essere configurato su altre porte fisiche.

9. Eliminare eventuali domini di broadcast vuoti dopo aver completato tutte le riparazioni delle porte:

   `network port broadcast-domain delete -broadcast-domain <broadcast_domain_name>`

10. verificare la raggiungibilità delle porte:

    `network port reachability show`

    Quando tutte le porte sono configurate correttamente e aggiunte ai domini di trasmissione corretti, il `network port reachability show` il comando deve riportare lo stato di raggiungibilità come `ok` per tutte le porte connesse e lo stato come `no-reachability` per porte senza connettività fisica. Se una delle porte riporta uno stato diverso da questi due, eseguire la riparazione della raggiungibilità e aggiungere o rimuovere le porte dai propri domini di trasmissione come indicato nella Fase 4.

11. Verificare che tutte le porte siano state inserite nei domini di broadcast:

    `network port show`

12. Verificare che tutte le porte nei domini di trasmissione abbiano configurato la MTU (Maximum Transmission Unit) corretta:

    `network port broadcast-domain show`

13. Ripristinare le porte LIF home, specificando le porte Vserver e LIF home, se presenti, che devono essere ripristinate seguendo questa procedura:

    a. Elencare eventuali LIF spostati:

       `displaced-interface show`

    b. Ripristinare i nodi home LIF e le porte home:

       `cluster controller-replacement network displaced-interface restore-home-node -node <node_name> -vserver <vserver_name> -lif-name <LIF_name>`

14. Verificare che tutte le LIF dispongano di una porta home e siano amministrativamente up:

    `network interface show -fields home-port, status-admin`

Ripristinare la configurazione del gestore delle chiavi sul node3

Se si utilizza NetApp Volume Encryption (NVE) e NetApp aggregate Encryption (NAE) per crittografare i volumi sul sistema che si sta aggiornando, la configurazione della crittografia deve essere sincronizzata con i nuovi nodi. Se non si sincronizza il gestore delle chiavi, quando si riposizionano gli aggregati node1 da node2 a node3 utilizzando ARL, potrebbero verificarsi errori perché node3 non dispone delle chiavi di crittografia necessarie per portare online volumi e aggregati crittografati.

A proposito di questa attività

Sincronizzare la configurazione della crittografia con i nuovi nodi seguendo questa procedura:

Fasi

1. Eseguire il seguente comando da node3:

   ```
   security key-manager onboard sync
   ```

2. Prima di spostare gli aggregati di dati, verificare che la chiave SVM-KEK sia stata ripristinata su "true" al nodo 3:

   ```
   ::> security key-manager key query -node node3 -fields restored -key
   -type SVM-KEK
   ```

   Esempio

   ```
   ::> security key-manager key query -node node3 -fields restored -key
   -type SVM-KEK

   node     vserver   key-server   key-id
   restored
   -------- --------- -----------  ----------------------------------------
   --------
   node3    svm1      ""           000000000000000020000000000a008a81976
   true
                                   2190178f9350e071fbb90f00000000000000000
   ```

Spostare gli aggregati non root e le LIF di dati NAS di proprietà del node1 da node2 a node3

Dopo aver verificato la configurazione di rete su node3 e prima di spostare gli aggregati da node2 a node3, è necessario verificare che i dati NAS LIF appartenenti al node1 che sono attualmente su node2 siano ricollocati da node2 a node3. È inoltre necessario verificare che le LIF SAN esistano sul node3.

A proposito di questa attività

Le LIF remote gestiscono il traffico verso le LUN SAN durante la procedura di aggiornamento. Lo spostamento

delle LIF SAN non è necessario per lo stato del cluster o del servizio durante l'aggiornamento. LE LIF SAN non vengono spostate a meno che non sia necessario mapparle su nuove porte. Dopo aver portato il nodo 3 online, verrete a verificare che i file LIF siano integri e posizionati sulle porte appropriate.

Fasi

1. Le LIF iSCSI trovano automaticamente le corrette porte home utilizzando la scansione della raggiungibilità. Le LIF SAN FC e NVMe/FC non si spostano automaticamente. Continuano a mostrare la porta home su cui si trovavano prima di eseguire l'aggiornamento.

   Verifica le LIF SAN su node3:

   a. Modifica di qualsiasi LIF SAN iSCSI che riporta uno stato operativo "inattivo" nelle nuove porte dati:

      ```
      network interface modify -vserver <vserver> -lif <iscsi_san_lif> admin down

      network interface modify -vserver <vserver> -lif <iscsi_san_lif> port
      <new_port> node <node>

      network interface modify -vserver <vserver> -lif <iscsi_san_lif>
      ```

   b. Modifica di qualsiasi LIF SAN FC e NVMe/FC che ospita il nuovo controller e segnala uno stato operativo "inattivo" alle porte FCP sul nuovo controller:

      ```
      network interface modify -vserver <vserver> -lif <fc_san_lif> admin down

      network interface modify -vserver <vserver> -lif <fc_san_lif> port
      <new_port> node <node>
      ```

   ```
   network interface modify -vserver <vserver> -lif <fc_san_lif>
   ```

2. Riprendere l'operazione di trasferimento:

   ```
   system controller replace resume
   ```

   Il sistema esegue le seguenti operazioni:

   - Verifica del quorum del cluster
   - Verifica dell'ID di sistema
   - Controllo della versione dell'immagine
   - Verifica della piattaforma di destinazione
   - Verifica della raggiungibilità della rete

   L'operazione viene interrotta in questa fase del controllo della raggiungibilità della rete.

3. Riprendere l'operazione di trasferimento:

   ```
   system controller replace resume
   ```

   Il sistema esegue i seguenti controlli:

   - Controllo dello stato del cluster
   - Controllo dello stato LIF del cluster

Dopo aver eseguito questi controlli, il sistema ricolloca gli aggregati non root e le LIF dei dati NAS di proprietà di node1 nel nuovo controller, node3. L'operazione di sostituzione del controller viene interrotta al termine del trasferimento delle risorse.

4. Controllare lo stato delle operazioni di trasferimento aggregato e LIF dei dati NAS:

   `system controller replace show-details`

   Se la procedura di sostituzione del controller è in pausa, controllare e correggere l'errore, se presente, quindi il problema `resume` per continuare l'operazione.

5. Se necessario, ripristinare e ripristinare eventuali LIF spostate. Elencare eventuali LIF spostate:

   `cluster controller-replacement network displaced-interface show`

   In caso di spostamento di LIF, ripristinare il nodo home al nodo node3:

   `cluster controller-replacement network displaced-interface restore-home-node`

6. Riprendere l'operazione per richiedere al sistema di eseguire i controlli successivi richiesti:

   `system controller replace resume`

   Il sistema esegue i seguenti post-controlli:

   - Verifica del quorum del cluster
   - Controllo dello stato del cluster
   - Controllo della ricostruzione degli aggregati
   - Controllo dello stato dell'aggregato
   - Controllo dello stato del disco
   - Controllo dello stato LIF del cluster
   - Controllo del volume

Fase 4. Spostare e dismettere il node2

Panoramica della fase 4

Durante la fase 4, è possibile spostare aggregati non root e LIF dati NAS da node2 a node3. Inoltre, registrare le informazioni necessarie per il node2 da utilizzare più avanti nella procedura, quindi dismettere il node2.

Fasi

1. "Spostare aggregati non root e LIF dati NAS da node2 a node3"
2. "Andare in pensione node2"

Spostare aggregati non root e LIF dati NAS da node2 a node3

Prima di sostituire il node2 con node4, spostare gli aggregati non root e le LIF dati NAS di proprietà di node2 in node3.

Prima di iniziare

Una volta completati i controlli successivi alla fase precedente, la release di risorse per node2 si avvia automaticamente. Gli aggregati non root e le LIF di dati non SAN vengono migrati da node2 a node3.

A proposito di questa attività

Le LIF remote gestiscono il traffico verso le LUN SAN durante la procedura di aggiornamento. Lo spostamento delle LIF SAN non è necessario per lo stato del cluster o del servizio durante l'aggiornamento.

Una volta migrati gli aggregati e i LIF, l'operazione viene sospesa per scopi di verifica. In questa fase, è necessario verificare se tutti gli aggregati non root e le LIF di dati non SAN vengono migrati in node3.

Il proprietario dell'abitazione per gli aggregati e le LIF non viene modificato; solo il proprietario corrente viene modificato.

Fasi

1. Verificare che tutti gli aggregati non root siano online e che il loro stato sia su node3:

   `storage aggregate show -node node3 -state online -root false`

   L'esempio seguente mostra che gli aggregati non root su node2 sono online:

   ```
   cluster::> storage aggregate show -node node3 state online -root false

   Aggregate      Size         Available   Used%   State   #Vols  Nodes
   RAID     Status
   ----------     ---------    ---------   ------  -----   -----  ------
   -------  ------
   aggr_1         744.9GB      744.8GB      0%     online  5      node2
   raid_dp  normal
   aggr_2         825.0GB      825.0GB      0%     online  1      node2
   raid_dp  normal
   2 entries were displayed.
   ```

   Se gli aggregati sono andati offline o diventano estranei sul node3, portarli online utilizzando il seguente comando sul node3, una volta per ogni aggregato:

   `storage aggregate online -aggregate aggr_name`

2. Verificare che tutti i volumi siano online sul nodo 3 utilizzando il seguente comando sul nodo 3 ed esaminando l'output:

   `volume show -node node3 -state offline`

   Se alcuni volumi sono offline sul node3, portarli online utilizzando il seguente comando sul node3, una volta per ogni volume:

   `volume online -vserver vserver_name -volume volume_name`

   Il *vserver_name* da utilizzare con questo comando si trova nell'output del precedente `volume show` comando.

3. Verificare che le LIF siano state spostate nelle porte corrette e che lo stato sia `up`. Se le LIF non sono attive, impostare lo stato amministrativo delle LIF su `up` Immettendo il seguente comando, una volta per ogni LIF:

   `network interface modify -vserver vserver_name -lif LIF_name -home-node node_name -status-admin up`

4. Se le porte che attualmente ospitano i file LIF dei dati non esistono sul nuovo hardware, rimuoverle dal dominio di trasmissione:

   `network port broadcast-domain remove-ports`

5. verificare che non vi siano dati LIF rimasti sul node2 immettendo il seguente comando ed esaminando l'output:

   `network interface show -curr-node node2 -role data`

Andare in pensione node2

Per dismettere il node2, chiudere il node2 correttamente e rimuoverlo dal rack o dallo chassis.

Fasi

1. Riprendere l'operazione:

   `system controller replace resume`

   Il nodo si arresta automaticamente.

Al termine

È possibile decommissionare il node2 una volta completato l'aggiornamento. Vedere "Decommissionare il vecchio sistema".

Fase 5. Installazione e boot node4

Panoramica della fase 5

Durante la fase 5, si installa e si avvia node4, si controlla che il cluster e le porte di gestione dei nodi da node2 siano online sul node4 e si verifica l'installazione node4. Se si utilizza NVE, si ripristina la configurazione del gestore delle chiavi. È inoltre possibile spostare le LIF dei dati NAS node2 e gli aggregati non root da node3 a node4 e verificare che le LIF SAN esistano sul node4.

Fasi

1. "Installazione e boot node4"
2. "Verificare l'installazione di node4"
3. "Ripristinare la configurazione del gestore delle chiavi sul nodo 4"
4. "Spostare gli aggregati non root e le LIF di dati NAS di proprietà di node2 da node3 a node4"

Installazione e boot node4

Si installa node4 nel rack, si trasferiscono le connessioni node2 a node4, si avvia node4 e si installa ONTAP. Quindi, si riassegnano i dischi di riserva di node2, gli eventuali dischi appartenenti al volume root e gli aggregati non root che non sono stati ricollocati a node3 nelle fasi precedenti del processo, come descritto in questa sezione.

A proposito di questa attività

L'operazione di trasferimento viene messa in pausa all'inizio di questa fase. Questo processo è per lo più automatizzato; l'operazione viene interrotta per consentirti di controllarne lo stato. È necessario riprendere manualmente l'operazione.

È necessario eseguire il netboot node4 se non dispone della stessa versione di ONTAP 9 installata sul node2. Dopo aver installato node4, avviarlo dall'immagine di ONTAP 9 memorizzata sul server Web. È quindi possibile scaricare i file corretti sul dispositivo di avvio per i successivi avviamenti del sistema, seguendo le istruzioni riportate in "Preparatevi per il netboot".

Fasi

1. assicurarsi che node4 disponga di spazio rack sufficiente.

   Se il nodo 4 si trova in uno chassis separato dal nodo 2, è possibile inserire il nodo 4 nella stessa posizione del nodo 3. Se node2 e node4 si trovano nello stesso chassis, node4 si trova già nella posizione rack appropriata.

2. Installare il nodo 4 nel rack seguendo le istruzioni contenute nelle *istruzioni di installazione e configurazione* relative al modello di nodo.
3. Nodo del cablo4, spostamento delle connessioni dal nodo 2 al nodo 4.

   Collegare i seguenti collegamenti seguendo le istruzioni contenute nelle *istruzioni di installazione e configurazione* o nei *requisiti e riferimenti per l'installazione della virtualizzazione FlexArray* per la piattaforma node4, il documento relativo allo shelf di dischi e *gestione dell'alta disponibilità*.

   Fare riferimento a. "Riferimenti" Per il collegamento ai *requisiti e riferimenti per l'installazione della virtualizzazione FlexArray* e alla *gestione dell'alta disponibilità*.

   - Console (porta di gestione remota)
   - Porte ha e cluster
   - Porte dati
   - Porte di gestione di cluster e nodi
   - Porte di storage Ethernet e SAS (Serial-Attached SCSI)
   - Configurazioni SAN: Porte switch iSCSI Ethernet, FC e NVMe/FC

Potrebbe essere necessario sostituire i cavi di interconnessione tra i controller vecchi e nuovi per consentire l'interoperabilità tra i diversi modelli di controller e di schede. Per una mappa dei cablaggi degli shelf di storage Ethernet dei sistemi in uso, fare riferimento alla "procedure di installazione del sistema" .

Per i controller introdotti in ONTAP 9.15.1 e versioni successive, il cluster e le interconnessioni ha utilizzano le stesse porte. Per le configurazioni con connessione da switch, è necessario collegare porte simili agli stessi switch del cluster. Ad esempio, quando si esegue l'upgrade a AFF A1K da un controller esistente, è necessario collegare E1a porte su entrambi i nodi a uno switch e e7a porte su entrambi i nodi al secondo switch.

4. Accendere il dispositivo al nodo 4, quindi interrompere il processo di avvio premendo `Ctrl-C` sul terminale della console per accedere al prompt dell'ambiente di boot.

   Quando si avvia node4, potrebbe essere visualizzato il seguente messaggio di avviso:

```
WARNING: The battery is unfit to retain data during a power outage. This
is likely
         because the battery is discharged but could be due to other
temporary
         conditions.
         When the battery is ready, the boot process will complete
         and services will be engaged. To override this delay, press 'c'
followed
         by 'Enter'
```

5. Se viene visualizzato il messaggio di avviso nella fase 4, eseguire le seguenti operazioni:

   a. Verificare la presenza di eventuali messaggi della console che potrebbero indicare un problema diverso da una batteria NVRAM in esaurimento e, se necessario, intraprendere le azioni correttive necessarie.

   b. Attendere che la batteria si ricarichi e che il processo di avvio venga completato.

   Attenzione: Non ignorare il ritardo; il mancato caricamento della batteria potrebbe causare la perdita di dati.

   Fare riferimento a. "Preparatevi per il netboot".

6. Configurare la connessione di netboot scegliendo una delle seguenti operazioni.

   È necessario utilizzare la porta di gestione e l'IP come connessione di netboot. Non utilizzare un IP LIF dei dati, altrimenti potrebbe verificarsi un'interruzione dei dati durante l'aggiornamento.

Se DHCP (Dynamic host Configuration Protocol) è…	Quindi…
In esecuzione	Configurare la connessione automaticamente utilizzando il seguente comando al prompt dell'ambiente di boot: `ifconfig e0M -auto`
Non in esecuzione	Configurare manualmente la connessione immettendo il seguente comando al prompt dell'ambiente di boot: `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain` *`filer_addr`* È l'indirizzo IP del sistema di storage (obbligatorio). *`netmask`* è la maschera di rete del sistema di storage (obbligatoria). *`gateway`* è il gateway per il sistema storage (obbligatorio). *`dns_addr`* È l'indirizzo IP di un name server sulla rete (opzionale). *`dns_domain`* È il nome di dominio DNS (opzionale). Potrebbero essere necessari altri parametri per l'interfaccia. Invio `help ifconfig` al prompt del firmware per ulteriori informazioni.

7. Eseguire il netboot al nodo 4:

   ```
   netboot http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz
   ```

   Il `<path_to_the_web-accessible_directory>` dovrebbe portare alla posizione in cui è stato scaricato `<ontap_version>_image.tgz` Nella fase 1 della sezione "Preparatevi per il netboot".

   Non interrompere l'avvio.

8. Dal menu di avvio, selezionare opzione `(7) Install new software first`.

   Questa opzione di menu consente di scaricare e installare la nuova immagine ONTAP sul dispositivo di avvio.

   Ignorare il seguente messaggio:

   ```
   This procedure is not supported for Non-Disruptive Upgrade on an HA pair
   ```

   La nota si applica agli aggiornamenti senza interruzioni di ONTAP e non agli aggiornamenti dei controller.

   Utilizzare sempre netboot per aggiornare il nuovo nodo all'immagine desiderata. Se si utilizza un altro metodo per installare l'immagine sul nuovo controller, l'immagine potrebbe non essere corretta. Questo problema riguarda tutte le versioni di ONTAP. La procedura di netboot combinata con l'opzione `(7) Install new software` Consente di cancellare il supporto di avvio e di posizionare la stessa versione di ONTAP su entrambe le partizioni dell'immagine.

9. Se viene richiesto di continuare la procedura, immettere `y`E quando viene richiesto il pacchetto, immettere l'URL:

```
http://<web_server_ip/path_to_web-
accessible_directory>/<ontap_version>_image.tgz
```

10. Completare i seguenti passaggi secondari per riavviare il modulo controller:
    a. Invio `n` per ignorare il ripristino del backup quando viene visualizzato il seguente prompt:

    ```
    Do you want to restore the backup configuration now? {y|n}
    ```

    b. Riavviare immettendo `y` quando viene visualizzato il seguente prompt:

    ```
    The node must be rebooted to start using the newly installed
    software. Do you want to reboot now? {y|n}
    ```

    Il modulo controller si riavvia ma si arresta al menu di avvio perché il dispositivo di avvio è stato riformattato e i dati di configurazione devono essere ripristinati.

11. Selezionare la modalità di manutenzione `5` dal menu di boot e premere `y` quando viene richiesto di continuare con l'avvio.
12. Verificare che il controller e lo chassis siano configurati come ha:

    `ha-config show`

    L'esempio seguente mostra l'output di `ha-config show` comando:

    ```
    Chassis HA configuration: ha
    Controller HA configuration: ha
    ```

    Il sistema registra in una PROM sia che si trovi in una coppia ha o in una configurazione standalone. Lo stato deve essere lo stesso su tutti i componenti all'interno del sistema standalone o della coppia ha.

13. Se il controller e lo chassis non sono configurati come ha, utilizzare i seguenti comandi per correggere la configurazione:

    `ha-config modify controller ha`

    `ha-config modify chassis ha`

14. Verificare che tutte le porte Ethernet utilizzate per il collegamento agli shelf Ethernet siano configurate come storage:

    `storage port show`

    L'output visualizzato dipende dalla configurazione del sistema. Il seguente esempio di uscita si riferisce a un nodo con una singola scheda di memoria in slot11. L'output del sistema potrebbe essere diverso:

```
*> storage port show
Port Type Mode    Speed(Gb/s) State    Status  VLAN ID
---- ---- ------- ----------- -------- ------- -------
e11a ENET storage 100 Gb/s    enabled  online  30
e11b ENET storage 100 Gb/s    enabled  online  30
```

15. Modificare le porte non impostate per la memorizzazione:

    `storage port modify -p <port> -m storage`

    Tutte le porte Ethernet collegate agli shelf di storage devono essere configurate come storage per consentire l'accesso ai dischi e agli shelf.

16. Uscire dalla modalità di manutenzione:

    `halt`

    Interrompere l'autoboot premendo Ctrl-C al prompt dell'ambiente di boot.

17. al node3, controllare la data, l'ora e il fuso orario del sistema:

    `date`

18. Al nodo 4, controllare la data utilizzando il seguente comando al prompt dell'ambiente di boot:

    `show date`

19. Se necessario, impostare la data sul node4:

    `set date <mm/dd/yyyy>`

20. In node4, controllare l'ora utilizzando il seguente comando al prompt dell'ambiente di boot:

    `show time`

21. Se necessario, impostare l'ora su node4:

    `set time <hh:mm:ss>`

22. Nel boot loader, impostare l'ID del sistema partner su node4:

    `setenv partner-sysid <node3_sysid>`

    Per il nodo 4, `partner-sysid` deve essere quello del node3.

    Salvare le impostazioni:

    `saveenv`

23. verificare `partner-sysid` per il nodo 4:

```
printenv partner-sysid
```

24. se sono installate unità di crittografia storage NetApp (NSE), procedere come segue.

> Se la procedura non è stata ancora eseguita, consultare l'articolo della Knowledge base "Come verificare se un disco è certificato FIPS" per determinare il tipo di unità con crittografia automatica in uso.

a. Impostare `bootarg.storageencryption.support` a. `true` oppure `false`.

Se i seguenti dischi sono in uso…	Quindi…
Unità NSE conformi ai requisiti di crittografia automatica FIPS 140-2 livello 2	`setenv bootarg.storageencryption.support` **`true`**
SED non FIPS di NetApp	`setenv bootarg.storageencryption.support` **`false`**

b. Accedere al menu di avvio speciale e selezionare l'opzione `(10) Set Onboard Key Manager recovery secrets`.

Inserire la passphrase e le informazioni di backup registrate in precedenza. Vedere "Gestire la crittografia dello storage utilizzando Onboard Key Manager".

25. Nodo di boot nel menu di boot:

```
boot_ontap menu.
```

26. su node4, vai al menu di avvio e usando 22/7, seleziona l'opzione nascosta `boot_after_controller_replacement`. Al prompt, immettere node2 per riassegnare i dischi di node2 a node4, come nell'esempio seguente.

Espandere l'esempio di output della console

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
.
<output truncated>
.
Please choose one of the following:
(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 22/7
(22/7)                          Print this secret List
(25/6)                          Force boot with multiple filesystem
disks missing.
(25/7)                          Boot w/ disk labels forced to clean.
(29/7)                          Bypass media errors.
(44/4a)                         Zero disks if needed and create new
flexible root volume.
(44/7)                          Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                        Clean all configuration on boot
device
(boot_after_controller_replacement) Boot after controller upgrade
```

```
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.
The boot device has changed. System configuration information could
be lost. Use option (6) to
restore the system configuration, or option (4) to initialize all
disks and setup a new system.
Normal Boot is prohibited.
Please choose one of the following:
(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? boot_after_controller_replacement
This will replace all flash-based configuration with the last backup
to disks. Are you sure
you want to continue?: yes
.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:
<nodename of the node being replaced>
Changing sysid of node node2 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
```

```
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote
    key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>
System rebooting...
.
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
.
.
<output truncated>
.
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
.
.
.
Login:
```

Nell'esempio di output della console precedente, ONTAP richiederà il nome del nodo partner se il sistema utilizza dischi di partizione avanzata dei dischi (ADP).

27. al prompt del CARICATORE, avviare:

```
boot_ontap menu
```

Ora, all'avvio, il nodo è in grado di rilevare tutti i dischi ad esso assegnati in precedenza e di avviarsi come previsto.

Quando i nodi del cluster che si stanno sostituendo utilizzano la crittografia dei volumi root, ONTAP non è in grado di leggere le informazioni sul volume dai dischi. Ripristinare le chiavi del volume root:

Se il volume root è crittografato, recupera i segreti di gestione delle chiavi integrati in modo che il sistema possa trovare il volume root.

a. Tornare al menu di avvio speciale:
`LOADER> boot_ontap menu`

```
Please choose one of the following:
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.

Selection (1-11)? 10
```

b. Selezionare **(10) Imposta segreti di ripristino di Onboard Key Manager**

c. Invio `y` al seguente prompt:

```
This option must be used only in disaster recovery procedures. Are you sure?
(y or n): y
```

d. Quando richiesto, inserire la passphrase del gestore delle chiavi.

e. Inserire i dati di backup quando richiesto.

> È necessario aver ottenuto la passphrase e i dati di backup in "Preparare i nodi per l'aggiornamento" sezione di questa procedura.

f. Dopo aver riavviato il sistema con lo speciale menu di boot, eseguire l'opzione **(1) Avvio normale**

> In questa fase potrebbe verificarsi un errore. Se si verifica un errore, ripetere i passaggi secondari in Passaggio 27 fino a quando il sistema non si avvia normalmente.

Verificare l'installazione di node4

È necessario verificare che le porte fisiche dal nodo 2 siano mappate correttamente alle porte fisiche sul nodo 4. In questo modo, il nodo 4 potrà comunicare con altri nodi del cluster e con la rete dopo l'aggiornamento.

A proposito di questa attività

Fare riferimento a. "Riferimenti" Per collegarsi a *Hardware Universe* per acquisire informazioni sulle porte sui nuovi nodi. Le informazioni verranno utilizzate più avanti in questa sezione.

Il layout fisico delle porte potrebbe variare a seconda del modello dei nodi. All'avvio del nuovo nodo, ONTAP tenterà di determinare quali porte dovrebbero ospitare le LIF del cluster per entrare automaticamente nel quorum.

Se le porte fisiche sul nodo 2 non vengono mappate direttamente alle porte fisiche sul nodo 4, consultare la sezione successiva Ripristinare la configurazione di rete sul nodo 4 deve essere utilizzato per riparare la connettività di rete.

Dopo aver installato e avviato il nodo 4, è necessario verificare che sia installato correttamente. È necessario attendere che il nodo 4 si unisca al quorum, quindi riprendere l'operazione di trasferimento.

A questo punto della procedura, l'operazione verrà messa in pausa quando node4 si unisce al quorum.

Fasi

1. Verificare che node4 si sia Unito al quorum:

   ```
   cluster show -node node4 -fields health
   ```

   L'output di `health` il campo deve essere `true`.

2. Verificare che node4 faccia parte dello stesso cluster di node3 e che sia integro:

   ```
   cluster show
   ```

3. Passare alla modalità avanzata dei privilegi:

   ```
   set advanced
   ```

4. Controllare lo stato dell'operazione di sostituzione del controller e verificare che sia in stato di pausa e nello stesso stato in cui si trovava prima dell'arresto del node2 per eseguire le attività fisiche di installazione di nuovi controller e cavi in movimento:

   ```
   system controller replace show
   ```

   ```
   system controller replace show-details
   ```

5. Riprendere l'operazione di sostituzione del controller:

   ```
   system controller replace resume
   ```

6. La sostituzione del controller viene interrotta per l'intervento con il seguente messaggio:

```
Cluster::*> system controller replace show
Node             Status                        Error-Action
---------------- ------------------------
-----------------------------------
Node2(now node4) Paused-for-intervention      Follow the instructions
given in
                                               Step Details
Node2

Step Details:
-------------------------------------------
To complete the Network Reachability task, the ONTAP network
configuration must be
manually adjusted to match the new physical network configuration of the
hardware.
This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For
detailed
commands and instructions, refer to the "Re-creating VLANs, ifgrps, and
broadcast
domains" section of the upgrade controller hardware guide for the ONTAP
version
running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show"
to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement
network displaced-vlans restore" to restore the VLAN on the desired
port.
2 entries were displayed.
```

In questa procedura, la sezione *Ricomposizione di VLAN, ifgrps e domini di trasmissione* è stata rinominata *Ripristino della configurazione di rete su node4*.

7. Con la sostituzione del controller in stato di pausa, passare alla sezione successiva di questo documento per ripristinare la configurazione di rete sul nodo.

Ripristinare la configurazione di rete sul nodo 4

Dopo aver confermato che il nodo 4 è in quorum e può comunicare con il nodo 3, verificare che le VLAN, i gruppi di interfacce e i domini di broadcast di node2 siano visibili sul nodo 4. Inoltre, verificare che tutte le porte di rete node4 siano configurate nei rispettivi domini di trasmissione corretti.

A proposito di questa attività

Per ulteriori informazioni sulla creazione e la ricreazione di VLAN, gruppi di interfacce e domini di trasmissione, fare riferimento a. "Riferimenti" Per collegarsi a *Network Management*.

Fasi

1. Elencare tutte le porte fisiche che si trovano sul nodo aggiorno2 (indicato come node4):

   ```
   network port show -node node4
   ```

   Vengono visualizzate tutte le porte di rete fisiche, le porte VLAN e le porte del gruppo di interfacce sul nodo. Da questo output è possibile visualizzare le porte fisiche spostate in `Cluster` Dominio di broadcast di ONTAP. È possibile utilizzare questo output per agevolare la scelta delle porte da utilizzare come porte membro del gruppo di interfacce, porte di base VLAN o porte fisiche standalone per l'hosting di LIF.

2. Elencare i domini di broadcast sul cluster:

   ```
   network port broadcast-domain show
   ```

3. Elencare la raggiungibilità delle porte di rete di tutte le porte sul nodo 4:

   ```
   network port reachability show
   ```

   L'output del comando è simile al seguente esempio:

```
ClusterA::*> network port reachability show
Node      Port     Expected Reachability                Reachability
Status
--------- -------- ----------------------------------
--------------------
node1_node3
          e0M      Default:Mgmt                        ok
          e10a     Default:Default                     ok
          e10b     -                                   no-reachability
          e10c     Default:Default                     ok
          e10d     -                                   no-reachability
          e1a      Cluster:Cluster                     ok
          e1b      -                                   no-reachability
          e7a      Cluster:Cluster                     ok
          e7b      -                                   no-reachability
node2_node4
          e0M      Default:Mgmt                        ok
          e10a     Default:Default                     ok
          e10b     -                                   no-reachability
          e10c     Default:Default                     ok
          e10d     -                                   no-reachability
          e1a      Cluster:Cluster                     ok
          e1b      -                                   no-reachability
          e7a      Cluster:Cluster                     ok
          e7b      -                                   no-reachability
18 entries were displayed.
```

Nell'esempio precedente, node2_node4 viene appena avviato dopo la sostituzione del controller. Dispone di diverse porte che non sono raggiungibilità e che sono in attesa di una scansione di raggiungibilità.

4. Ripristina la raggiungibilità di ciascuna porta sul nodo 4 con uno stato di raggiungibilità diverso da `ok`. Eseguire il seguente comando, prima su qualsiasi porta fisica, quindi su qualsiasi porta VLAN, una alla volta:

   `network port reachability repair -node <node_name> -port <port_name>`

   L'output è simile al seguente esempio:

```
Cluster ::> reachability repair -node node2_node4 -port e10a
```

```
Warning: Repairing port "node2_node4: e10a" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

Un messaggio di avviso, come mostrato sopra, è previsto per le porte con uno stato di raggiungibilità che potrebbe essere diverso dallo stato di raggiungibilità del dominio di trasmissione in cui si trova attualmente.

Esaminare la connettività della porta e rispondere `y` oppure `n` a seconda dei casi.

Verificare che tutte le porte fisiche abbiano la raggiungibilità prevista:

```
network port reachability show
```

Quando viene eseguita la riparazione della raggiungibilità, ONTAP tenta di posizionare le porte nei domini di trasmissione corretti. Tuttavia, se non è possibile determinare la raggiungibilità di una porta e non appartiene a nessuno dei domini di broadcast esistenti, ONTAP creerà nuovi domini di broadcast per queste porte.

5. Se la configurazione del gruppo di interfacce non corrisponde al layout della porta fisica del nuovo controller, modificarla seguendo la procedura riportata di seguito.

   a. È necessario innanzitutto rimuovere le porte fisiche che devono essere porte membro del gruppo di interfacce dall'appartenenza al dominio di trasmissione. Per eseguire questa operazione, utilizzare il seguente comando:

      ```
      network port broadcast-domain remove-ports -broadcast-domain
      <broadcast_domain_name> -ports <node_name:port_name>
      ```

   b. Aggiungere una porta membro a un gruppo di interfacce:

      ```
      network port ifgrp add-port -node <node_name> -ifgrp <ifgrp> -port
      <port_name>
      ```

   c. Il gruppo di interfacce viene aggiunto automaticamente al dominio di trasmissione circa un minuto dopo l'aggiunta della prima porta membro.

   d. Verificare che il gruppo di interfacce sia stato aggiunto al dominio di trasmissione appropriato:

      ```
      network port reachability show -node <node_name> -port <ifgrp>
      ```

      Se lo stato di raggiungibilità del gruppo di interfacce non è `ok`, assegnarlo al dominio di trasmissione appropriato:

```
network port broadcast-domain add-ports -broadcast-domain
<broadcast_domain_name> -ports <node:port>
```

6. Assegnare le porte fisiche appropriate a `Cluster` dominio di broadcast:

   a. Determinare quali porte hanno la raggiungibilità di `Cluster` dominio di broadcast:

      ```
      network port reachability show -reachable-broadcast-domains Cluster:Cluster
      ```

   b. Riparare qualsiasi porta con la possibilità di accedere a `Cluster` dominio di broadcast, se il suo stato di raggiungibilità non è `ok`:

      ```
      network port reachability repair -node <node_name> -port <port_name>
      ```

7. Spostare le restanti porte fisiche nei domini di trasmissione corretti utilizzando uno dei seguenti comandi:

```
network port reachability repair -node <node_name> -port <port_name>

network port broadcast-domain remove-port

network port broadcast-domain add-port
```

Verificare che non siano presenti porte irraggiungibili o impreviste. Verificare lo stato di raggiungibilità di tutte le porte fisiche utilizzando il comando seguente ed esaminare l'output per confermare lo stato `ok`:

```
network port reachability show -detail
```

8. Ripristinare eventuali VLAN che potrebbero essere state spostate seguendo la procedura riportata di seguito:

   a. Elenco VLAN spostate:

      ```
      cluster controller-replacement network displaced-vlans show
      ```

      Viene visualizzato un output simile al seguente:

      ```
      Cluster::*> displaced-vlans show
      (cluster controller-replacement network displaced-vlans show)
                  Original
      Node        Base Port     VLANs
      ---------   ---------     --------------
      Node1       a0a           822, 823
                  e10a          822, 823
      ```

   b. Ripristinare le VLAN spostate dalle porte di base precedenti:

      ```
      cluster controller-replacement network displaced-vlans restore
      ```

      Di seguito viene riportato un esempio di ripristino delle VLAN spostate dal gruppo di interfaccia a0a allo stesso gruppo di interfacce:

      ```
      Cluster::*> displaced-vlans restore -node node2_node4 -port a0a
      -destination-port a0a
      ```

      Di seguito viene riportato un esempio di ripristino delle VLAN spostate sulla porta "e10a" in "e10b":

      ```
      Cluster::*> displaced-vlans restore -node node2_node4 -port e10a
      -destination-port e10b
      ```

      Quando un ripristino della VLAN ha esito positivo, le VLAN spostate vengono create sulla porta di destinazione specificata. Il ripristino della VLAN non riesce se la porta di destinazione è membro di un gruppo di interfacce o se la porta di destinazione non è disponibile.

Attendere circa un minuto per inserire le VLAN appena ripristinate nei domini di trasmissione appropriati.

a. Creare nuove porte VLAN in base alle necessità per le porte VLAN non presenti in `cluster controller-replacement network displaced-vlans show` ma deve essere configurato su altre porte fisiche.

9. Eliminare eventuali domini di broadcast vuoti dopo aver completato tutte le riparazioni delle porte:

   ```
   network port broadcast-domain delete -broadcast-domain <broadcast_domain_name>
   ```

10. Verificare la raggiungibilità delle porte:

    ```
    network port reachability show
    ```

    Quando tutte le porte sono configurate correttamente e aggiunte ai domini di trasmissione corretti, il `network port reachability show` il comando deve riportare lo stato di raggiungibilità come `ok` per tutte le porte connesse e lo stato come `no-reachability` per porte senza connettività fisica. Se una delle porte riporta uno stato diverso da questi due, eseguire la riparazione della raggiungibilità e aggiungere o rimuovere le porte dai propri domini di trasmissione come indicato in Fase 4.

11. Verificare che tutte le porte siano state inserite nei domini di broadcast:

    ```
    network port show
    ```

12. Verificare che tutte le porte nei domini di trasmissione abbiano configurato la MTU (Maximum Transmission Unit) corretta:

    ```
    network port broadcast-domain show
    ```

13. Ripristinare le porte LIF home, specificando le porte Vserver e LIF home, se presenti, che devono essere ripristinate:

    a. Elencare eventuali LIF spostati:

       ```
       displaced-interface show
       ```

    b. Ripristinare le porte LIF home:

       ```
       displaced-interface restore-home-node -node <node_name> -vserver
       <vserver_name> -lif-name <LIF_name>
       ```

14. Verificare che tutte le LIF dispongano di una porta home e siano amministrativamente up:

    ```
    network interface show -fields home-port, status-admin
    ```

Ripristinare la configurazione del gestore delle chiavi sul nodo 4

Se si utilizza NetApp Volume Encryption (NVE) e NetApp aggregate Encryption (NAE) per crittografare i volumi sul sistema che si sta aggiornando, la configurazione della crittografia deve essere sincronizzata con i nuovi nodi. Se non si sincronizza il gestore delle chiavi, quando si riposizionano gli aggregati node2 da node3 a node4 utilizzando ARL, potrebbero verificarsi errori perché node4 non dispone delle chiavi di crittografia necessarie per portare online volumi e aggregati crittografati.

A proposito di questa attività

Sincronizzare la configurazione della crittografia con i nuovi nodi seguendo questa procedura:

Fasi

1. Eseguire il seguente comando da node4:

   ```
   security key-manager onboard sync
   ```

2. Prima di spostare gli aggregati di dati, verificare che la chiave SVM-KEK sia ripristinata su "true" in node4:

   ```
   ::> security key-manager key query -node node4 -fields restored -key
   -type SVM-KEK
   ```

   Esempio

   ```
   ::> security key-manager key query -node node4 -fields restored -key
   -type SVM-KEK

   node     vserver   key-server   key-id
   restored
   -------- --------- -----------  ----------------------------------------
   --------
   node4    svm1      ""           000000000000000002000000000000a008a81976
   true
                                   2190178f9350e071fbb90f00000000000000000
   ```

Spostare gli aggregati non root e le LIF di dati NAS di proprietà di node2 da node3 a node4

Dopo aver verificato la configurazione di rete sul nodo 4 e prima di spostare gli aggregati dal nodo 3 al nodo 4, è necessario verificare che i dati NAS LIF appartenenti al nodo 2 che sono attualmente sul nodo 3 vengano ricollocati dal nodo 3 al nodo 4. È inoltre necessario verificare che le LIF SAN esistano sul node4.

A proposito di questa attività

Le LIF remote gestiscono il traffico verso le LUN SAN durante la procedura di aggiornamento. Lo spostamento delle LIF SAN non è necessario per lo stato del cluster o del servizio durante l'aggiornamento. LE LIF SAN non vengono spostate a meno che non sia necessario mapparle su nuove porte. Dopo aver portato il nodo 4 online, verrete a verificare che i file LIF siano integri e posizionati sulle porte appropriate.

Fasi

1. Le LIF iSCSI trovano automaticamente le corrette porte home utilizzando la scansione della raggiungibilità. Le LIF SAN FC e NVMe/FC non si spostano automaticamente. Continuano a mostrare la porta home su cui si trovavano prima di eseguire l'aggiornamento.

   Verifica le LIF SAN su node4:

   a. Modifica di qualsiasi LIF SAN iSCSI che riporta uno stato operativo "inattivo" nelle nuove porte dati:

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> admin down

network interface modify -vserver <vserver> -lif <iscsi_san_lif> port
<new_port> node <node>

network interface modify -vserver <vserver> -lif <iscsi_san_lif>
```

b. Modifica di qualsiasi LIF SAN FC e NVMe/FC che ospita il nuovo controller e segnala uno stato operativo "inattivo" alle porte FCP sul nuovo controller:

```
network interface modify -vserver <vserver> -lif <fc_san_lif> admin down

network interface modify -vserver <vserver> -lif <fc_san_lif> port
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif>
```

2. Riprendere l'operazione di trasferimento:

```
system controller replace resume
```

Il sistema esegue le seguenti operazioni:

- Verifica del quorum del cluster
- Verifica dell'ID di sistema
- Controllo della versione dell'immagine
- Verifica della piattaforma di destinazione
- Verifica della raggiungibilità della rete

L'operazione viene interrotta in questa fase del controllo della raggiungibilità della rete.

3. Riprendere l'operazione di trasferimento:

```
system controller replace resume
```

Il sistema esegue i seguenti controlli:

- Controllo dello stato del cluster
- Controllo dello stato LIF del cluster

Dopo aver eseguito questi controlli, il sistema ricolloca gli aggregati non root e le LIF dei dati NAS di proprietà di node2 nel nuovo controller, node4. L'operazione di sostituzione del controller viene interrotta al termine del trasferimento delle risorse.

4. Controllare lo stato delle operazioni di trasferimento aggregato e LIF dei dati NAS:

```
system controller replace show-details
```

Se la procedura di sostituzione del controller è in pausa, controllare e correggere l'errore, se presente, quindi il problema `resume` per continuare l'operazione.

5. Se necessario, ripristinare e ripristinare eventuali LIF spostate. Elencare eventuali LIF spostate:

```
cluster controller-replacement network displaced-interface show
```

Se i file LIF vengono spostati, ripristinare il nodo home al nodo node4:

```
cluster controller-replacement network displaced-interface restore-home-node
```

6. Riprendere l'operazione per richiedere al sistema di eseguire i controlli successivi richiesti:

```
system controller replace resume
```

Il sistema esegue i seguenti post-controlli:

- Verifica del quorum del cluster
- Controllo dello stato del cluster
- Controllo della ricostruzione degli aggregati
- Controllo dello stato dell'aggregato
- Controllo dello stato del disco
- Controllo dello stato LIF del cluster
- Controllo del volume

Fase 6. Completare l'aggiornamento

Panoramica della fase 6

Durante la fase 6, confermi che i nuovi nodi sono impostati correttamente e, se i nuovi nodi sono abilitati per la crittografia, configuri e configuri Storage Encryption o NetApp Volume Encryption. È inoltre necessario decommissionare i vecchi nodi e riprendere le operazioni di SnapMirror.

Fasi

1. "Gestire l'autenticazione utilizzando i server KMIP"
2. "Verificare che i nuovi controller siano impostati correttamente"
3. "Impostare Storage Encryption sul nuovo modulo controller"
4. "Impostare NetApp Volume o aggregate Encryption sul nuovo modulo controller"
5. "Decommissionare il vecchio sistema"
6. "Riprendere le operazioni di SnapMirror"

Gestire l'autenticazione utilizzando i server KMIP

Puoi utilizzare i server KMIP (Key Management Interoperability Protocol) per gestire le chiavi di autenticazione.

Fasi

1. Aggiungere un nuovo controller:

```
security key-manager external enable
```

2. Aggiungere il gestore delle chiavi:

   ```
   security key-manager external add-servers -key-servers
   key_management_server_ip_address
   ```

3. Verificare che i server di gestione delle chiavi siano configurati e disponibili per tutti i nodi del cluster:

   ```
   security key-manager external show-status
   ```

4. Ripristinare le chiavi di autenticazione da tutti i server di gestione delle chiavi collegati al nuovo nodo:

   ```
   security key-manager external restore -node new_controller_name
   ```

Verificare che i nuovi controller siano impostati correttamente

Per confermare la corretta configurazione, è necessario attivare la coppia ha. È inoltre necessario verificare che node3 e node4 possano accedere reciprocamente allo storage e che non siano in possesso di LIF dei dati appartenenti ad altri nodi del cluster. Inoltre, devi confermare che node3 possiede gli aggregati di node1 e che node4 possiede gli aggregati di node2 e che i volumi per entrambi i nodi sono online.

Fasi

1. Dopo i controlli post-node2, vengono attivate la coppia di ha cluster e failover dello storage per il cluster node2. Al termine dell'operazione, entrambi i nodi vengono visualizzati come completati e il sistema esegue alcune operazioni di pulizia.
2. Verificare che il failover dello storage sia attivato:

   ```
   storage failover show
   ```

   L'esempio seguente mostra l'output del comando quando è attivato il failover dello storage:

   ```
   cluster::> storage failover show
                       Takeover
   Node     Partner  Possible   State Description
   -------- -----    -------    ------------------
   node3    node4    true       Connected to node4
   node4    node3    true       Connected to node3
   ```

3. Verificare che node3 e node4 appartengano allo stesso cluster utilizzando il seguente comando ed esaminando l'output:

   ```
   cluster show
   ```

4. Verificare che node3 e node4 possano accedere reciprocamente allo storage utilizzando il seguente comando ed esaminando l'output:

   ```
   storage failover show -fields local-missing-disks, partner-missing-disks
   ```

5. Verificare che né node3 né node4 detengano le LIF dei dati di proprietà di altri nodi del cluster utilizzando il

seguente comando ed esaminando l'output:

```
network interface show
```

Se nessuno dei nodi 3 o node4 possiede le LIF dei dati di proprietà di altri nodi del cluster, ripristinare le LIF dei dati al proprietario di casa:

```
network interface revert
```

6. Verificare che node3 possieda gli aggregati dal node1 e che node4 possieda gli aggregati dal node2:

```
storage aggregate show -owner-name <node3>
```

```
storage aggregate show -owner-name <node4>
```

7. Determinare se i volumi sono offline:

```
volume show -node <node3> -state offline
```

```
volume show -node <node4> -state offline
```

8. Se alcuni volumi non sono in linea, confrontarli con l'elenco dei volumi non in linea acquisito nella sezione "Preparare i nodi per l'aggiornamento"e portare online uno qualsiasi dei volumi offline, come richiesto, utilizzando il seguente comando, una volta per ciascun volume:

```
volume online -vserver <vserver_name> -volume <volume_name>
```

9. Installare nuove licenze per i nuovi nodi utilizzando il seguente comando per ciascun nodo:

```
system license add -license-code <license_code,license_code,license_code…>
```

Il parametro License-code accetta un elenco di 28 chiavi alfabetiche maiuscole. È possibile aggiungere una licenza alla volta oppure più licenze contemporaneamente, separando ciascuna chiave di licenza con una virgola.

10. Rimuovere tutte le vecchie licenze dai nodi originali utilizzando uno dei seguenti comandi:

```
system license clean-up -unused -expired
```

```
system license delete -serial-number <node_serial_number> -package
<licensable_package>
```

- Eliminare tutte le licenze scadute:

  ```
  system license clean-up -expired
  ```

- Eliminare tutte le licenze inutilizzate:

  ```
  system license clean-up -unused
  ```

- Eliminare una licenza specifica da un cluster utilizzando i seguenti comandi sui nodi:

  ```
  system license delete -serial-number <node1_serial_number> -package *
  ```

```
system license delete -serial-number <node2_serial_number> -package *
```

Viene visualizzato il seguente output:

```
Warning: The following licenses will be removed:
<list of each installed package>
Do you want to continue? {y|n}: y
```

Invio `y` per rimuovere tutti i pacchetti.

11. Verificare che le licenze siano installate correttamente utilizzando il seguente comando ed esaminando l'output:

    ```
    system license show
    ```

    È possibile confrontare l'output con quello acquisito nella sezione "Preparare i nodi per l'aggiornamento".

12. se nella configurazione vengono utilizzati dischi con crittografia automatica e la variabile è stata impostata `kmip.init.maxwait` su `off` (ad esempio, in "Installazione e boot node4, passaggio 24"), è necessario annullare l'impostazione della variabile:

    ```
    set diag; systemshell -node <node_name> -command sudo kenv -u -p
    kmip.init.maxwait
    ```

13. configurare gli SP utilizzando il seguente comando su entrambi i nodi:

    ```
    system service-processor network modify -node <node_name>
    ```

    Fare riferimento a. "Riferimenti" Per informazioni dettagliate sul sistema, consultare il documento *riferimento amministrazione sistema* e i comandi di *ONTAP 9.8: Riferimento pagina manuale* `service-processor network modify` comando.

14. Se si desidera configurare un cluster senza switch sui nuovi nodi, fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp* e seguire le istruzioni in *passaggio a un cluster senza switch a due nodi*.

Al termine

Se Storage Encryption è attivato su node3 e node4, completare la sezione "Impostare Storage Encryption sul nuovo modulo controller". In caso contrario, completare la sezione "Decommissionare il vecchio sistema".

Impostare Storage Encryption sul nuovo modulo controller

Se il controller sostituito o il partner ha del nuovo controller utilizza Storage Encryption, è necessario configurare il nuovo modulo controller per Storage Encryption, inclusa l'installazione dei certificati SSL e la configurazione dei server di gestione delle chiavi.

A proposito di questa attività

Questa procedura include i passaggi che vengono eseguiti sul nuovo modulo controller. Immettere il comando sul nodo corretto.

Fasi

1. Verificare che i server di gestione delle chiavi siano ancora disponibili, che il loro stato e le relative informazioni sulla chiave di autenticazione:

   ```
   security key-manager external show-status

   security key-manager onboard show-backup
   ```

2. Aggiungere i server di gestione delle chiavi elencati nel passaggio precedente all'elenco dei server di gestione delle chiavi nel nuovo controller.

   a. Aggiungere il server di gestione delle chiavi:

      ```
      security key-manager external add-servers -key-servers
      key_management_server_ip_address
      ```

   b. Ripetere il passaggio precedente per ciascun server di gestione delle chiavi elencato. È possibile collegare fino a quattro server di gestione delle chiavi.

   c. Verificare che i server di gestione delle chiavi siano stati aggiunti correttamente:

      ```
      security key-manager external show
      ```

3. Sul nuovo modulo controller, eseguire la configurazione guidata della gestione delle chiavi per configurare e installare i server di gestione delle chiavi.

   È necessario installare gli stessi server di gestione delle chiavi installati sul modulo controller esistente.

   a. Avviare la configurazione guidata del server di gestione delle chiavi sul nuovo nodo:

      ```
      security key-manager external enable
      ```

   b. Completare la procedura guidata per configurare i server di gestione delle chiavi.

4. Ripristinare le chiavi di autenticazione da tutti i server di gestione delle chiavi collegati al nuovo nodo:

   ```
   security key-manager external restore -node new_controller_name
   ```

Impostare NetApp Volume o aggregate Encryption sul nuovo modulo controller

Se il controller sostituito o il partner ad alta disponibilità (ha) del nuovo controller utilizza NetApp Volume Encryption (NVE) o NetApp aggregate Encryption (NAE), è necessario configurare il nuovo modulo controller per NVE o NAE.

A proposito di questa attività

Questa procedura include i passaggi che vengono eseguiti sul nuovo modulo controller. Immettere il comando sul nodo corretto.

Gestione delle chiavi integrata

Configurare NVE o NAE utilizzando Onboard Key Manager.

Fasi

1. Ripristinare le chiavi di autenticazione da tutti i server di gestione delle chiavi collegati al nuovo nodo:

   ```
   security key-manager onboard sync
   ```

Gestione esterna delle chiavi

Configurare NVE o NAE utilizzando External Key Management.

Fasi

1. Verificare che i server di gestione delle chiavi siano ancora disponibili, che il loro stato e le relative informazioni sulla chiave di autenticazione:

   ```
   security key-manager key query -node node
   ```

2. Aggiungere i server di gestione delle chiavi elencati nel passaggio precedente all'elenco dei server di gestione delle chiavi nel nuovo controller:

   a. Aggiungere il server di gestione delle chiavi:

      ```
      security key-manager external add-servers -key-servers
      key_management_server_ip_address
      ```

   b. Ripetere il passaggio precedente per ciascun server di gestione delle chiavi elencato. È possibile collegare fino a quattro server di gestione delle chiavi.

   c. Verificare che i server di gestione delle chiavi siano stati aggiunti correttamente:

      ```
      security key-manager external show
      ```

3. Sul nuovo modulo controller, eseguire la configurazione guidata della gestione delle chiavi per configurare e installare i server di gestione delle chiavi.

   È necessario installare gli stessi server di gestione delle chiavi installati sul modulo controller esistente.

   a. Avviare la configurazione guidata del server di gestione delle chiavi sul nuovo nodo:

      ```
      security key-manager external enable
      ```

   b. Completare la procedura guidata per configurare i server di gestione delle chiavi.

4. Ripristinare le chiavi di autenticazione da tutti i server di gestione delle chiavi collegati al nuovo nodo:

   ```
   security key-manager external restore
   ```

   Questo comando richiede la passphrase OKM

   Per ulteriori informazioni, consultare l'articolo della Knowledge base "Come ripristinare la configurazione del server di gestione delle chiavi esterne dal menu di avvio di ONTAP".

Al termine

Controllare se i volumi sono stati portati offline perché le chiavi di autenticazione non erano disponibili o non è stato possibile raggiungere i server EKM. Ripristinare i volumi online utilizzando `volume online` comando.

Decommissionare il vecchio sistema

Dopo l'aggiornamento, è possibile decommissionare il vecchio sistema tramite il NetApp Support Site. La disattivazione del sistema indica a NetApp che il sistema non è più in funzione e lo rimuove dai database di supporto.

Fasi

1. Fare riferimento a. "Riferimenti" Per collegarsi al *sito di supporto NetApp* ed effettuare l'accesso.
2. Selezionare **prodotti > prodotti** dal menu.
3. Nella pagina **Visualizza sistemi installati**, scegliere i **criteri di selezione** da utilizzare per visualizzare le informazioni sul sistema.

   È possibile scegliere una delle seguenti opzioni per individuare il sistema:

   - Numero di serie (situato sul retro dell'unità)
   - Numeri di serie per la mia posizione
4. Selezionare **Go!**

   Una tabella visualizza le informazioni sul cluster, inclusi i numeri di serie.
5. Individuare il cluster nella tabella e selezionare **Decommissionare questo sistema** dal menu a discesa Product Tool Set (Set strumenti prodotto).

Riprendere le operazioni di SnapMirror

È possibile riprendere i trasferimenti di SnapMirror che sono stati disattivati prima dell'aggiornamento e riprendere le relazioni di SnapMirror. Gli aggiornamenti sono programmati una volta completato l'aggiornamento.

Fasi

1. Verificare lo stato di SnapMirror sulla destinazione:

   ```
   snapmirror show
   ```
2. Riprendere la relazione di SnapMirror:

   ```
   snapmirror resume -destination-vserver vserver_name
   ```

Risolvere i problemi

Risolvere i problemi

Si potrebbe riscontrare un errore durante l'aggiornamento della coppia di nodi. Il nodo potrebbe bloccarsi, gli aggregati potrebbero non spostarsi o i LIF potrebbero non migrare.

La causa dell'errore e la relativa soluzione dipendono dal momento in cui si è verificato l'errore durante la procedura di aggiornamento.

Fare riferimento alla tabella che descrive le diverse fasi della procedura nella sezione "Panoramica dell'aggiornamento ARL". Le informazioni sugli errori che possono verificarsi sono elencate in base alla fase della procedura.

Errori di trasferimento aggregati

Il trasferimento di aggregati (ARL) potrebbe non riuscire in diversi punti durante l'aggiornamento.

Verificare la presenza di errori di trasferimento degli aggregati

Durante la procedura, l'ARL potrebbe non funzionare nella fase 2, 3 o 5.

Fasi

1. Immettere il seguente comando ed esaminare l'output:

   ```
   storage aggregate relocation show
   ```

   Il `storage aggregate relocation show` il comando mostra quali aggregati sono stati riallocati correttamente e quali no, insieme alle cause del guasto.

2. Verificare la presenza di eventuali messaggi EMS nella console.
3. Eseguire una delle seguenti operazioni:

   - Intraprendere l'azione correttiva appropriata, a seconda dell'output di `storage aggregate relocation show` E l'output del messaggio EMS.
   - Forzare il trasferimento dell'aggregato o degli aggregati utilizzando `override-vetoes` o il `override-destination-checks` opzione di `storage aggregate relocation start` comando.

   Per informazioni dettagliate su `storage aggregate relocation start`, `override-vetoes`, e. `override-destination-checks` opzioni, fare riferimento a. "Riferimenti" Per collegarsi ai comandi di *ONTAP 9.8: Manuale riferimento pagina*.

Gli aggregati originalmente sul node1 sono di proprietà del node4 dopo il completamento dell'upgrade

Al termine della procedura di aggiornamento, node3 dovrebbe essere il nuovo nodo home degli aggregati che in origine aveva node1 come nodo home. È possibile trasferirli dopo l'aggiornamento.

A proposito di questa attività

Gli aggregati potrebbero non riuscire a riallocare correttamente, avendo node1 come nodo principale invece di node3 nelle seguenti circostanze:

- Durante la fase 3, quando gli aggregati vengono ricollocati dal nodo 2 al nodo 3. Alcuni degli aggregati che vengono ricollocati hanno node1 come nodo principale. Ad esempio, un tale aggregato potrebbe essere chiamato aggr_node_1. Se il trasferimento di aggr_node_1 non riesce durante la fase 3 e non è possibile forzare il trasferimento, l'aggregato verrà lasciato indietro al nodo 2.
- Dopo la fase 4, quando il node2 viene sostituito con il node4. Quando node2 viene sostituito, aggr_node_1

verrà online con node4 come nodo home invece di node3.

Una volta attivato il failover dello storage, è possibile risolvere il problema di proprietà non corretto dopo la fase 6, attenendosi alla seguente procedura:

Fasi

1. Immettere il seguente comando per ottenere un elenco di aggregati:

   `storage aggregate show -nodes node4 -is-home true`

   Per identificare gli aggregati che non sono stati correttamente ricollocati, fare riferimento all'elenco degli aggregati con il proprietario di casa del node1 ottenuto nella sezione "Preparare i nodi per l'aggiornamento" e confrontarlo con l'output del comando precedente.

2. Confrontare l'output del passaggio 1 con l'output acquisito per il nodo 1 nella sezione "Preparare i nodi per l'aggiornamento" e annotare eventuali aggregati che non sono stati correttamente ricollocati.
3. spostare gli aggregati rimasti al nodo 4:

   `storage aggregate relocation start -node node4 -aggr aggr_node_1 -destination node3`

   Non utilizzare `-ndo-controller-upgrade` durante questa riallocazione.

4. Verificare che node3 sia ora il proprietario domestico degli aggregati:

   `storage aggregate show -aggregate aggr1,aggr2,aggr3… -fields home-name`

   aggr1,aggr2,aggr3… è l'elenco degli aggregati che avevano il node1 come proprietario di casa originale.

   Gli aggregati che non hanno node3 come proprietario di casa possono essere ricollocati in node3 utilizzando lo stesso comando di rilocazione in Fase 3.

Riavvio, panic o cicli di alimentazione

Il sistema potrebbe bloccarsi (riavvio, panico o ciclo di alimentazione) durante diverse fasi dell'aggiornamento.

La soluzione a questi problemi dipende da quando si verificano.

Si riavvia, esegue il panic o si accende durante la fase di pre-controllo

Node1 o node2 si blocca prima della fase di pre-check con la coppia ha ancora attivata

Se il nodo 1 o il nodo 2 si bloccano prima della fase di pre-controllo, non è stato ancora trasferito alcun aggregato e la configurazione della coppia ha è ancora abilitata.

A proposito di questa attività

Il takeover e il giveback possono procedere normalmente.

Fasi

1. Controllare la console per i messaggi EMS che il sistema potrebbe aver emesso e adottare l'azione

correttiva consigliata.

2. Continuare con la procedura di aggiornamento della coppia di nodi.

Riavvio, panic o cicli di alimentazione durante la prima fase di rilascio delle risorse

Node1 si blocca durante la prima fase di resource-release con la coppia ha ancora attivata

Alcuni o tutti gli aggregati sono stati ricollocati da node1 a node2 e la coppia ha è ancora abilitata. Node2 prende il controllo del volume root del node1 e di qualsiasi aggregato non root che non sia stato trasferito.

A proposito di questa attività

La proprietà degli aggregati che sono stati ricollocati è uguale alla proprietà degli aggregati non root che sono stati presi in consegna perché il proprietario di casa non è cambiato.

Quando nod1 entra in `waiting for giveback` state, node2 restituisce tutti gli aggregati non root node1.

Fasi

1. Dopo l'avvio di node1, tutti gli aggregati non root di node1 sono tornati a node1. È necessario eseguire un trasferimento manuale degli aggregati dal nodo 1 al nodo 2:
   `storage aggregate relocation start -node node1 -destination node2 -aggregate -list * -ndocontroller-upgrade true`
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Node1 si blocca durante la prima fase di resource-release mentre la coppia ha è disattivata

Node2 non prende il controllo, ma sta ancora fornendo dati da tutti gli aggregati non root.

Fasi

1. Far salire il node1.
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Node2 si guasta durante la prima fase di resource-release con la coppia ha ancora attivata

Node1 ha trasferito alcuni o tutti i suoi aggregati al node2. La coppia ha è attivata.

A proposito di questa attività

Node1 prende il controllo di tutti gli aggregati del node2 e di qualsiasi aggregato che aveva trasferito al node2. All'avvio di node2, il trasferimento dell'aggregato viene completato automaticamente.

Fasi

1. Alzati il node2.
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Node2 si blocca durante la prima fase di resource-release e dopo la disattivazione della coppia ha

Node1 non prende il posto.

Fasi

1. Alzati il node2.

   Un'interruzione del client si verifica per tutti gli aggregati mentre node2 è in fase di avvio.

2. Continuare con il resto della procedura di aggiornamento della coppia di nodi.

Riavvio, panic o cicli di alimentazione durante la prima fase di verifica

Node2 si blocca durante la prima fase di verifica con la coppia ha disattivata

Node3 non prende il controllo in seguito a un crash node2 in quanto la coppia ha è già disattivata.

Fasi

1. Alzati il node2.

   Un'interruzione del client si verifica per tutti gli aggregati mentre node2 è in fase di avvio.

2. Continuare con la procedura di aggiornamento della coppia di nodi.

Node3 si blocca durante la prima fase di verifica con la coppia ha disattivata

Node2 non prende il controllo, ma sta ancora fornendo dati da tutti gli aggregati non root.

Fasi

1. Alzati il node3.
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Riavvio, panic o cicli di alimentazione durante la prima fase di recupero delle risorse

Node2 si blocca durante la prima fase di recupero delle risorse durante il trasferimento degli aggregati

Node2 ha riallocato alcuni o tutti i suoi aggregati dal node1 al node3. Node3 fornisce i dati degli aggregati che sono stati ricollocati. La coppia ha è disattivata e quindi non c'è alcun Takeover.

A proposito di questa attività

Esiste un'interruzione del client per gli aggregati che non sono stati ricollocati. All'avvio di node2, gli aggregati di node1 vengono ricollocati in node3.

Fasi

1. Alzati il node2.
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Node3 si blocca durante la prima fase di recupero delle risorse durante il trasferimento degli aggregati

Se node3 si blocca mentre node2 sta spostando gli aggregati in node3, l'attività continua dopo l'avvio di node3.

A proposito di questa attività

Node2 continua a servire gli aggregati rimanenti, ma gli aggregati che erano già stati ricollocati in node3 incontrano un'interruzione del client durante l'avvio di node3.

Fasi

1. Alzati il node3.
2. Continuare con l'aggiornamento del controller.

Riavvio, panic o cicli di alimentazione durante la fase di post-controllo

Node2 o node3 si bloccano durante la fase post-check

La coppia ha è disattivata, quindi non si tratta di un Takeover. Si verifica un'interruzione del client per gli aggregati appartenenti al nodo che ha riavviato il sistema.

Fasi

1. Richiamare il nodo.
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Riavvio, panic o cicli di alimentazione durante la seconda fase di rilascio delle risorse

Node3 si blocca durante la seconda fase di rilascio delle risorse

Se node3 si blocca mentre node2 sta spostando gli aggregati, l'attività continua dopo l'avvio di node3.

A proposito di questa attività

Node2 continua a servire gli aggregati rimanenti, ma gli aggregati già ricollocati negli aggregati di node3 e node3 incontrano interruzioni del client durante l'avvio di node3.

Fasi

1. Alzati il node3.
2. Continuare con la procedura di aggiornamento del controller.

Node2 si blocca durante la seconda fase di rilascio delle risorse

Se il nodo 2 si blocca durante il trasferimento dell'aggregato, il nodo 2 non viene sostituito.

A proposito di questa attività

Node3 continua a servire gli aggregati che sono stati ricollocati, ma gli aggregati di proprietà di node2 incontrano interruzioni dei client.

Fasi

1. Alzati il node2.
2. Continuare con la procedura di aggiornamento del controller.

Riavvio, panic o cicli di alimentazione durante la seconda fase di verifica

Node3 si blocca durante la seconda fase di verifica

Se node3 si blocca durante questa fase, il takeover non avviene perché la coppia ha è già disattivata.

A proposito di questa attività

Si verifica un'interruzione del client per tutti gli aggregati fino al riavvio del node3.

Fasi

1. Alzati il node3.
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Node4 si blocca durante la seconda fase di verifica

Se node4 si blocca durante questa fase, il takeover non si verifica. Node3 fornisce i dati degli aggregati.

A proposito di questa attività

Esiste un'interruzione per gli aggregati non root che sono stati già ricollocati fino al riavvio del node4.

Fasi

1. Far salire il node4.
2. Continuare con la procedura di aggiornamento della coppia di nodi.

Problemi che possono verificarsi in più fasi della procedura

Alcuni problemi possono verificarsi durante diverse fasi della procedura.

Output imprevisto del comando "show di failover dello storage"

Durante la procedura, se il nodo che ospita tutti gli aggregati di dati viene avviato accidentalmente o viene riavviato, potrebbe essere visualizzato un output imprevisto per `storage failover show` comando prima e dopo il riavvio, il panico o il ciclo di alimentazione.

A proposito di questa attività

Potrebbe essere visualizzato un output imprevisto da `storage failover show` Comando in fase 2, fase 3, fase 4 o fase 5.

L'esempio seguente mostra l'output previsto di `storage failover show` comando se non ci sono riavvii o panic sul nodo che ospita tutti gli aggregati di dati:

```
cluster::> storage failover show

                    Takeover
Node     Partner    Possible  State Description
-------  ---------  --------- -----------------
node1    node2      false     Unknown
node2    node1      false     Node owns partner aggregates as part of the
non-disruptive head upgrade procedure. Takeover is not possible: Storage
failover is disabled.
```

L'esempio seguente mostra l'output di `storage failover show` comando dopo un riavvio o un panic:

```
cluster::> storage failover show

                    Takeover
Node      Partner   Possible  State Description
--------  --------  --------- -----------------
node1     node2     -         Unknown
node2     node1     false     Waiting for node1, Partial giveback, Takeover
is not possible: Storage failover is disabled
```

Sebbene l'output indichi che un nodo è in giveback parziale e che il failover dello storage è disattivato, è possibile ignorare questo messaggio.

Fasi

Non è richiesta alcuna azione; continuare con la procedura di aggiornamento della coppia di nodi.

Errore di migrazione LIF

Dopo la migrazione, i file LIF potrebbero non essere disponibili online dopo la migrazione in fase 2, fase 3 o fase 5.

Fasi

1. Verificare che la dimensione MTU della porta sia uguale a quella del nodo di origine.

   Ad esempio, se la dimensione MTU della porta del cluster è 9000 sul nodo di origine, dovrebbe essere 9000 sul nodo di destinazione.

2. Controllare la connettività fisica del cavo di rete se lo stato fisico della porta è `down`.

Riferimenti

Quando si eseguono le procedure di questo contenuto, potrebbe essere necessario consultare il contenuto di riferimento o visitare i siti Web di riferimento.

- Contenuto di riferimento
- Siti di riferimento

Contenuto di riferimento

I contenuti specifici di questo aggiornamento sono elencati nella tabella seguente.

Contenuto	Descrizione
"Panoramica sull'amministrazione con la CLI"	Descrive come amministrare i sistemi ONTAP, illustra come utilizzare l'interfaccia CLI, come accedere al cluster, come gestire i nodi e molto altro ancora.
"Decidere se utilizzare Gestore di sistema o l'interfaccia utente di ONTAP per la configurazione del cluster"	Descrive come configurare ONTAP.

Contenuto	Descrizione
"Gestione di dischi e aggregati con CLI"	Descrive come gestire lo storage fisico ONTAP utilizzando la CLI. Mostra come creare, espandere e gestire gli aggregati, come lavorare con gli aggregati di Flash Pool, come gestire i dischi e come gestire le policy RAID.
"Requisiti e riferimenti per l'installazione della virtualizzazione FlexArray"	Contiene istruzioni sul cablaggio e altre informazioni per i sistemi di virtualizzazione FlexArray.
"Gestione dell'alta disponibilità"	Descrive come installare e gestire le configurazioni in cluster ad alta disponibilità, tra cui failover dello storage e takeover/giveback.
"Gestione dello storage logico con la CLI"	Descrive come gestire in modo efficiente le risorse di storage logico, utilizzando volumi, volumi FlexClone, file e LUN, Volumi FlexCache, deduplica, compressione, qtree e quote.
"Upgrade ed espansione di MetroCluster"	Vengono fornite procedure per l'aggiornamento dei modelli di controller e storage nella configurazione MetroCluster, la transizione da una configurazione MetroCluster FC a una configurazione MetroCluster IP e l'espansione della configurazione MetroCluster mediante l'aggiunta di nodi aggiuntivi.
"Gestione della rete"	Descrive come configurare e gestire le porte di rete fisiche e virtuali (VLAN e gruppi di interfacce), i LIF, il routing e i servizi di risoluzione degli host nei cluster; ottimizza il traffico di rete mediante il bilanciamento del carico; monitora il cluster utilizzando SNMP.
"Comandi di ONTAP 9.13.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.13.1 supportati.
"Comandi di ONTAP 9.14.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.14.1 supportati.
"Comandi di ONTAP 9.15.1: Guida alla pagina"	Descrive la sintassi e l'utilizzo dei comandi ONTAP 9.15.1 supportati.
"Gestione SAN con CLI"	Descrive come configurare e gestire LUN, igroups e destinazioni utilizzando i protocolli iSCSI e FC, nonché spazi dei nomi e sottosistemi utilizzando il protocollo NVMe/FC.
"Riferimento alla configurazione SAN"	Contiene informazioni sulle topologie FC e iSCSI e sugli schemi di cablaggio.
"Eseguire l'upgrade spostando volumi o storage"	Descrive come aggiornare rapidamente l'hardware del controller in un cluster spostando lo storage o i volumi. Descrive inoltre come convertire un modello supportato in uno shelf di dischi.
"Aggiornare ONTAP"	Contiene le istruzioni per scaricare e aggiornare ONTAP.
"Utilizzare i comandi "System controller replace" per aggiornare i modelli di controller nello stesso chassis"	Descrive le procedure di trasferimento degli aggregati necessarie per aggiornare un sistema senza interruzioni, mantenendo il vecchio chassis e i dischi del sistema.

Contenuto	Descrizione
"Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller con ONTAP 9.8 o versione successiva"	Descrive le procedure di trasferimento degli aggregati necessarie per l'aggiornamento senza interruzioni dei controller che eseguono ONTAP 9.8 utilizzando i comandi "system controller replace".
"Utilizzare il trasferimento di aggregati per aggiornare manualmente l'hardware del controller con ONTAP 9.8 o versione successiva"	Descrive le procedure di trasferimento degli aggregati necessarie per eseguire aggiornamenti manuali dei controller senza interruzioni con ONTAP 9.8 o versione successiva.

Siti di riferimento

Il "Sito di supporto NetApp" Contiene inoltre documentazione sulle schede di interfaccia di rete (NIC) e su altri componenti hardware che potrebbero essere utilizzati con il sistema. Contiene anche "Hardware Universe", che fornisce informazioni sull'hardware supportato dal nuovo sistema.

Accesso "Documentazione di ONTAP 9".

Accedere a. "Active IQ Config Advisor" tool.

Informazioni sul copyright

Informazioni sul marchio commerciale